UNIVERSIDAD DE BUENOS AIRES
Facultad de Ciencias Exactas y Naturales
Departamento de Matemática

Skew braces: estructura y algunas aplicaciones

Tesis presentada para optar al título de Doctor de la Universidad de Buenos Aires
en el área Ciencias Matemáticas

Emiliano Francisco Acri

Director de tesis: Dr. Leandro Vendramin
Consejero de estudios: Dr. Daniel Perrucci

Buenos Aires, 2024

Resumen

Skew braces: estructura y algunas aplicaciones

En esta tesis estudiamos propiedades de la estructura conocida como *skew brace*. Específicamente, nos centramos en aquellas que tienen grupo aditivo nilpotente y generalizamos algunas propiedades conocidas del caso abeliano. Las skew braces han cobrado una gran relevancia en los últimos años gracias a la conexión existente entre ellas y las soluciones de la ecuación conjuntista de Yang–Baxter (EYB). Toda solución no degenerada de la EYB tiene asociada una estructura de braza en sobre su grupo de estructura.

Debido a esta conexión, hemos dirigido nuestros esfuerzos a la clasificación y construcción de skew braces de ciertos órdenes. Específicamente, hemos construido las skew braces de orden pq y p^2q para números primos distintos p y q. Para ello es necesario conocer todos los grupos del orden requerido y conseguir todos los subgrupos regulares del holomorfo de cada uno de los grupos. A partir de la lista de subgrupos regulares hemos contado clases de conjugación bajo la acción del grupo de automorfismos del grupo dado.

Palabras clave: skew braces, ecuación de Yang–Baxter, soluciones conjuntistas, grupo de Bieberbach, propiedad de producto único

Abstract

Skew braces: structure and some applications

In this thesis we study properties of the structure known as *skew brace*. Specifically, we focus on those with a nilpotent additive group and generalize some known properties of the abelian case. Skew braces have gained great relevance in recent years thanks to the connection between them and the solutions to the set-theoretic Yang-Baxter equation. Every non-degenerate solution of the Yang–Baxter equation has an associated skew brace structure on its structure group.

Due to this connection, we have directed our efforts to the classification and construction of skew braces of certain orders. Specifically, we have constructed skew braces of order pq and p^2q for distinct prime numbers p and q. To do so, it is necessary to know all the groups of the required order and to obtain all the regular subgroups of the holomorph of each of the groups. From the list of regular subgroups we have counted conjugacy classes under the action of the automorphism group of the given group.

Keywords: skew braces, Yang–Baxter equation, set-theoretic solutions, Bieberbach groups, unique product property

Índice general

Índice de tablas

Agradecimientos

Introducción

A lo largo de los últimos años se ha despertado un fuerte interés en el estudio de la llamada *ecuación de Yang–Baxter*, específicamente en la versión conjuntista propuesta por Drinfel'd en [30] a comienzos de los años ′90. Se trata de pares (X, r) donde X es un conjunto y $r : X \times X \to X \times X$ es una función de conjuntos que satisface la relación

$$(r \times \mathrm{id})(\mathrm{id} \times r)(r \times \mathrm{id}) = (\mathrm{id} \times r)(r \times \mathrm{id})(\mathrm{id} \times r).$$

Sobre el fin del siglo pasado se comenzó a estudiar en forma sistemática a las soluciones de la versión conjuntista. Cabe señalar aquí los trabajos fundacionales de [31, 39, 49, 64]. En su trabajo [55] de 2007, Rump presenta una estructura algebraica que permite construir soluciones *involutivas* de la ecuación de Yang–Baxter: él la denomina *brace*. Se trata de una generalización de los anillos radicales en el sentido de Jacobson, una estructura que Rump observó que permite construir soluciones. Gracias a su aporte se consigue construir una enorme cantidad de ejemplos de soluciones a partir de la construcción de *braces* y esta estructura consigue un interés en sí misma.

En el año 2017, Guarnieri y Vendramin en [41], inspirados en el trabajo de Rump, dan una generalización de la estructura de *braces* que denominan *skew braces*. Esta estructura permite construir soluciones no involutivas llevando más lejos el estudio realizado por Rump previamente.

Gracias a la estructura de *skew brace* se han observado conexiones entre la ecuación de Yang–Baxter y la teoría de anillos, variedades planas, ordenabilidad de grupos, teoría de Garside, entre otros (algunos ejemplos pueden verse en [12, 25, 26, 28, 34, 38, 57]).

A lo largo de esta tesis iremos introduciendo distintas estructuras asociadas a las soluciones de la ecuación de Yang–Baxter y a las *skew braces* (brazas torcidas).

Esta tesis es el resultado del trabajo de investigación que publiqué por partes en cuatro *papers*, veánse [1–4]. El trabajo está organizado de la siguiente forma:

- En la primera parte presentamos los conceptos básicos sobre brazas torcidas que forman el objeto principal de estudio de esta tesis. También mencionamos la conexión con las soluciones de la ecuación de Yang–Baxter.

- En la segunda parte trabajamos con una familia específica de soluciones de la ecuación de Yang–Baxter: las soluciones retractables. Recordamos los concep-

tos de nilpotencia a izquierda y a derecha de una braza torcida y demostramos una representación lineal del grupo de estructura asociado a una solución involutiva finita. Esta representación nos será especialmente útil para poder demostar el Teorema 2.4.7 referido a la propiedad de producto único en grupos.

Además, definimos una noción de p-nilpotencia a izquierda y a derecha para brazas torcidas de tipo nilpotente. Esto nos permitió mejorar algunos resultados de [50].

- En la tercera parte nos enfocamos en la clasificación de brazas torcidas de distintos órdenes.

  - En el capítulo 3 clasificamos las brazas torcidas de orden pq con p y q números primos distintos. Para obtener la clasificación utilizamos la conexión existente entre brazas torcidas de tipo A y subgrupos regulares de $\mathrm{Hol}(A)$, el grupo holomorfo de A.
  - En los capítulos 4 y 5 nos enfocamos en la clasificación de brazas torcidas de orden p^2q donde p y q son dos números primos distintos. Para ello, hemos dividido el análisis según el tipo de grupo aditivo de las brazas torcidas. En el capítulo 4 asumiremos que las brazas torcidas son de tipo abeliano y en el capítulo 5 asumiremos que son de tipo no abeliano. A lo largo del análisis iremos incluyendo tablas que nos permitirán resumir el trabajo realizado en cada una de las secciones.

    Como aplicación de todos los resultados conseguidos damos una demostración a una conjetura sobre la cantidad de brazas torcidas de orden p^2q.

Parte 1

Brazas torcidas y estructuras asociadas

Capítulo 1

Conceptos básicos

Este capítulo tiene el doble propósito de presentar las definiciones y los conceptos básicos que serán utilizados a lo largo de esta tesis y el de fijar la notación que utilizaremos en la mayor parte del trabajo. Cualquier notación adicional que necesitemos en el futuro y no merezca ser incluida como hecho general en este capítulo, será oportunamente clarificada.

1.1. Ecuación conjuntista de Yang–Baxter

Comencemos con la versión conjuntista de la *ecuación de Yang–Baxter* (**EYB**). Ésta fue formulada por Drinfeld en [30]. Diremos que un par (X, r) donde X es un conjunto y $r\colon X \times X \to X \times X$ es una función biyectiva es una *solución* de la ecuación de Yang–Baxter si se satisface la identidad:

$$(r \times \mathrm{id})(\mathrm{id} \times r)(r \times \mathrm{id}) = (\mathrm{id} \times r)(r \times \mathrm{id})(\mathrm{id} \times r). \qquad (\mathbf{EYB})$$

El problema de hallar soluciones para esta ecuación es demasiado grande para poder atacarse en su generalidad. Para aproximarnos a este problema, utilizaremos métodos combinatorios. Para ello, consideraremos una clase especial de soluciones a lo largo de todo el trabajo: las *soluciones no degeneradas*. Se trata de soluciones biyectivas que pueden escribirse de la forma:

$$r(x, y) = (\sigma_x(y), \tau_y(x)), \quad x, y \in X,$$

donde σ_x, τ_y son permutaciones del conjunto X; es decir, $\sigma_x, \tau_y \in \mathbb{S}_X$ cualesquiera sean $x, y \in X$. De ahora en adelante, cuando nos refiramos a una *solución*, se tratará siempre de una *solución no degenerada*.

Un ejemplo simple de solución no degenerada es el de Lyubashenko.

Ejemplo 1.1.1 (Lyubashenko)**.** Si σ y τ son dos permutaciones de X que conmutan entre sí, entonces $r(x, y) = (\sigma(y), \tau(x))$ es una solución no degenerada de la **EYB**.

Los primeros trabajos relacionados al estudio de soluciones de la **EYB** fueron los de Etingof, Schedler y Soloviev, [31], y Gateva-Ivanova y Van den Bergh, [39].

Ambos trabajos consideran *soluciones involutivas*, es decir, aquellas que cumplen $r^2 = \mathrm{id}_{X\times X}$.

En [55], Rump observó que un anillo radical R da lugar a una solución involutiva. Aquí, debe entenderse *anillo radical* en el sentido de Jacobson; es decir, R es un anillo tal que el conjunto subyacente con la operación $x \circ y = x + y + xy$ es un grupo.

A partir de esta observación, Rump introdujo una nueva estructura algebraica que generaliza la estructura de anillo radical dando un marco algebraico para poder estudiar soluciones involutivas: las *brazas*[1].

Para construir soluciones involutivas, Etingof *et al.* introdujeron la noción de *solución retractable*, [31]. Dada una solución involutiva (X, r), definimos una relación sobre el conjunto X de la siguiente manera:

$$x \sim y \quad \text{si y solo si} \quad \sigma_x = \sigma_y.$$

Esta relación resulta ser de equivalencia. Nos queda, entonces, una solución bien definida sobre el conjunto de clases de equivalencia $X/\!\sim$. A esta solución se la conoce como la *retracción* de la solución (X, r) y la notaremos por $\mathrm{Ret}(X, r)$. Dado que la retracción sigue siendo una solución involutiva, podemos definir inductivamente la n-ésima retracción de la siguiente manera: $\mathrm{Ret}^1(X, r) = \mathrm{Ret}(X, r)$ y $\mathrm{Ret}^{n+1}(X, r) = \mathrm{Ret}(\mathrm{Ret}^n(X, r))$ para todo $n \geq 1$.

Diremos que una solución es *irretractable* si $\mathrm{Ret}(X, r) = (X, r)$ y diremos que es una *multipermutación* si existe un n tal que $\mathrm{Ret}^n(X, r)$ tiene un solo elemento. Podemos decir que las multipermutaciones generalizan las soluciones de Lyubashenko (Ejemplo 1.1.1). Las soluciones involutivas por multipermutaciones recibieron mucha atención en los últimos años (podemos citar por ejemplo: [11,12,20,35,37,58,60,62]).

Muchas de las ideas utilizadas para estudiar las soluciones involutivas pueden transportarse al contexto de las soluciones no involutivas. Las brazas definidas por Rump y utilizadas para el estudio de soluciones involutivas fueron generalizadas a *skew braces* y utilizadas para soluciones no involutivas.

De esta forma, es casi obligada la comprensión de la estructura de *skew brace*.

1.2. Brazas (torcidas)

Una *braza torcida a izquierda*[2] es una terna $(A, +, \circ)$ tal que $(A, +)$ y $(A, \circ)$ son grupos (no necesariamente abelianos, la notación quedará clara en breve) que satisfacen la compatibilidad dada por

$$a \circ (b + c) = a \circ b - a + a \circ c$$

cualesquiera sean los elementos $a, b, c \in A$. La operación de suma $+$ precede a la operación de multiplicación $\circ$ como es usual.

Claramente, utilizamos la notación $-a$ para referirnos al inverso de un elemento $a \in A$ con respecto a la operación $+$. Notaremos por a' al inverso de ese mismo elemento pero con respecto a la operación $\circ$.

[1] *Braces* en el original.

[2] *Skew left brace* en el original.

Observación 1.2.1. Si notamos por 1_+ y $1_\circ$ a los elementos neutros para las operaciones $+$ y $\circ$ respectivamente entonces podemos ver que $1_+ = 1_\circ$. En efecto, a partir de la compatibilidad tenemos que

$$\begin{aligned} 1_\circ \circ (1_\circ + 1_\circ) &= 1_\circ \circ 1_\circ - 1_\circ + 1_\circ \circ 1_\circ \\ 1_\circ + 1_\circ &= \underbrace{1_\circ - 1_\circ}_{=1_+} + 1_\circ \\ 1_\circ &= 1_+ \end{aligned}$$

Si bien concentraremos este trabajo en las brazas torcidas a izquierda, se puede definir una noción de *braza torcida a derecha* de forma completamente análoga modificando la compatibilidad anterior por

$$(b + c) \circ a = b \circ a - a + c \circ a.$$

A lo largo de este trabajo surgirán una buena cantidad de ejemplos de brazas torcidas a izquierda pero aquí referimos algunos para familiarizarnos con la definición.

Ejemplo 1.2.2 (Braza trivial)**.** Dado cualquier grupo $(A, +)$, definimos la operación $\circ$ como $a \circ b := a + b$.

Ejemplo 1.2.3. Consideremos el conjunto $G = \{g_j : j \in \mathbb{Z}/6\mathbb{Z}\}$ y definamos las operaciones

$$g_i + g_j = g_{i+(-1)^i j}, \qquad g_i \circ g_j = g_{i+j}.$$

Es fácil verificar que ambas operaciones le dan a G una estructura de grupo y que $-g_i = g_{(-1)^{i+1} i}$. Ahora bien

$$\begin{aligned} g_i \circ g_j - g_i + g_i \circ g_k &= g_{i+j} - g_i + g_{i+k} \\ &= g_{i+j} + g_{(-1)^{i+1} i} + g_{i+k} \\ &= g_{i+j+(-1)^{i+j}(-1)^{i+1} i} + g_{i+k} \\ &= g_l \end{aligned}$$

donde

$$\begin{aligned} l &= i + j + (-1)^{i+j}(-1)^{i+1} i + (-1)^{i+j+(-1)^{i+j}(-1)^{i+1} i}(i + k) \\ &= i + j + (-1)^{j+1} i + (-1)^{i+j+(-1)^{j+1} i}(i + k) \\ &= i + j + (-1)^{j+1} i + (-1)^{i(1+(-1)^{j+1})+j}(i + k) \\ &= i + j + (-1)^{j+1} i + (-1)^{j}(i + k) \\ &= i + j + (-1)^{j} k. \end{aligned}$$

Luego

$$g_l = g_{i+j+(-1)^j k} = g_i \circ g_{j+(-1)^j k} = g_i \circ (g_j + g_k).$$

Al igual que en el estudio de otras estructuras algebraicas (tales como grupos o anillos), contamos con nociones de morfismos e ideales. A continuación resumimos las ideas básicas que utilizaremos a lo largo de nuestro trabajo.

Definición 1.2.4. Si $(B_1, +_1, \circ_1)$ y $(B_2, +_2, \circ_2)$ son dos brazas torcidas y $f : B_1 \to B_2$ es una función de conjuntos, decimos que f es un *morfismo de brazas torcidas* si se satisfacen las condiciones

- $f(a +_1 b) = f(a) +_2 f(b)$
- $f(a \circ_1 b) = f(a) \circ_2 f(b)$

cualesquiera sean $a, b \in B_1$.

Como es usual, si un morfismo f es biyectivo, diremos que se trata de un *isomorfismo* y dos brazas torcidas serán *isomorfas* si existe un isomorfismo entre ellas.

El estudio de brazas torcidas en general es bastante amplio, razón por la cual se suelen estudiar familias teniendo en cuenta alguna propiedad adicional sobre la estructura aditiva, es decir sobre $(A, +)$. Si denotamos por $\mathcal{X}$ a una propiedad aplicable a un grupo (por ejemplo abeliano, nilpotente, resoluble, etc.), diremos que una braza torcida es de tipo $\mathcal{X}$ si el grupo aditivo pertenece a la clase $\mathcal{X}$.

Las brazas definidas por Rump que referimos anteriormente son las brazas torcidas de tipo abeliano.

Para una braza torcida A podemos definir un morfismo de grupos

$$\lambda : (A, \circ) \to \mathrm{Aut}(A, +), \quad a \mapsto \lambda_a$$

donde $\lambda_a(b) = -a + a \circ b$. Denotaremos a su núcleo como $\ker \lambda$, como es usual.

Por definición, tenemos que

$$a \circ b = a + \lambda_a(b), \qquad a + b = a \circ \lambda_a^{-1}(b), \qquad \lambda_a(a') = -a.$$

Una operación muy útil a la hora de estudiar brazas torcidas es la siguiente:

$$a * b = \lambda_a(b) - b.$$

Cualesquiera sean $a, b, c \in A$, se cumple que

$$a * (b + c) = a * b + b + a * c - b,$$
$$(a \circ b) * c = a * (b * c) + b * c + a * c.$$

El siguiente ejemplo nos muestra de qué forma surgen las brazas como una generalización de la estructura de anillo.

Ejemplo 1.2.5. Sea $(R, +, *)$ un anillo radical en el sentido de Jacobson, es decir que la operación $a \circ b = a + a * b + b$ define una estructura de grupo sobre el conjunto R. Entonces $(R, +, \circ)$ es una braza como se puede comprobar inmediatamente a partir de la definición.

Notemos que $a * b$ resulta ser igual a $-a + a \circ b - b$ que es lo que definimos como

Definición 1.2.6. Una *bi-braza torcida* es una braza torcida $(A, +, \circ)$ tal que $(A, \circ, +)$ también es una braza torcida (véase [23]). Equivalentemente,

$$x + (y \circ z) = (x + y) \circ x' \circ (x + z) \tag{1.1}$$

se satisface cualesquiera sean $x, y, z \in A$.

1.3. Estructuras algebraicas asociadas a la ecuación de Yang–Baxter

En esta sección resumiremos las estructuras algebraicas básicas que se pueden asociar a una solución de la ecuación de Yang–Baxter.

Dada una solución involutiva (X, r), se puede definir lo que se conoce como el *grupo de estructura* $G(X, r)$ de la solución. Este grupo fue definido en [31, 49, 64] como el grupo generado por los elementos $x \in X$ y las relaciones

$$x \circ y = u \circ v \quad \text{donde} \quad r(x, y) = (u, v).$$

El uso de $\circ$ para denotar la operación del grupo $G(X, r)$ no es caprichoso, en breve veremos que sobre este grupo puede definirse una estructura de braza torcida.

Para el caso de soluciones involutivas finitas, el grupo $G(X, r)$ resulta ser libre de torsión (véase por ejemplo [39]). En [24] se probó que $G(X, r)$ es un grupo de Garside.

Siguiendo con el caso involutivo, tenemos un segundo grupo que puede asociarse a una solución dada: el *grupo de permutaciones* $\mathcal{G}(X, r)$ que es el subgrupo de $\mathbb{S}_X$ (el grupo simétrico sobre el conjunto X) generado por $\{\sigma_x : x \in X\}$. Claramente, $\mathcal{G}(X, r)$ actúa sobre X y si X es finito, entonces $\mathcal{G}(X, r)$ es finito.

1.4. Relación entre brazas torcidas y soluciones de la ecuación de Yang–Baxter

Si $(A, +, \circ)$ es una braza torcida, entonces la función

$$r_A : A \times A \to A \times A, \quad r_A(a, b) = \big(\lambda_a(b), \lambda_a(b)' \circ a \circ b\big)$$

es una solución de la **EYB**.

Más aún, esta solución es involutiva (es decir $r_A^2 = \mathrm{id}_{A \times A}$) si y sólo si A es una braza torcida de tipo abeliano (es decir, una braza como las definidas por Rump).

Recíprocamente, si (X, r) es una solución entonces el grupo de estructura $G(X, r)$ admite una única estructura de braza torcida que satisface la identidad

$$r_{G(X,r) \times G(X,r)}(\iota \times \iota) = (\iota \times \iota) r$$

donde $\iota : X \to G(X,r)$ es la función canónica (recordemos que los generadores de $G(X,r)$ son los elementos de X). Cabe aclarar que, en general, esta inclusión no es inyectiva.

Adicionalmente, la braza torcida $G(X,r)$ satisface una propiedad universal. Si A es cualquier braza torcida y $f : X \to A$ es una función que satisface la identidad $r_A(f \times f) = (f \times f)r$, entonces existe un único $\varphi : G(X,r) \to A$ morfismo de brazas torcidas tal que $\varphi\iota = f$ y $r_A(\varphi \times \varphi) = (\varphi \times \varphi)r_{G(X,r)}$. Resultados similares pueden encontrarse en [31, 49, 64].

Notemos que el grupo multiplicativo de la braza torcida $G(X,r)$ es el grupo de estructura que definimos sobre la solución (X,r) en la Sección 1.3.

El grupo de permutaciones $\mathcal{G}(X,r)$ de una solución involutiva admite una estructura de braza definiendo la operación

$$\lambda_a + \lambda_b = \lambda_a \lambda_{\lambda_a^{-1}(b)}$$

cualesquiera sean $a, b \in A$. Este resultado puede consultarse en [10]. Para una versión para el caso no involutivo, véase [9].

Un *ideal a izquierda* de una braza torcida es un subgrupo de la estructura aditiva que es estable bajo la acción de λ. Se sigue que un ideal a izquierda resulta ser un subgrupo de la estructura multiplicativa.

Un *ideal* es un ideal a izquierda que además es un subgrupo normal tanto del grupo aditivo como del multiplicativo. Decimos que una braza torcida A no nula es *simple* si tiene solamente dos ideales (los triviales $\{0\}$ y A).

El *zócalo* de una braza torcida A es el ideal $\mathrm{Soc}(A) = \ker\lambda \cap Z(A,+)$, donde denotamos al centro del grupo aditivo por $Z(A,+)$.

El conjunto

$$\mathrm{Fix}(A) = \{a \in A : \lambda_x(a) = a \text{ para todo } x \in A\}$$

es claramente un ideal a izquierda.

Parte 2

Soluciones retractables de la EYB

Capítulo 2

Retractabilidad de soluciones y p-nilpotencia de brazas torcidas

Los resultados de este capítulo están basados en el trabajo [4] en el que exploramos la relación entre las soluciones retractables y una cierta noción de nilpotencia sobre las brazas torcidas. Recuperaremos algunos hechos conocidos sobre brazas nilpotentes y los extenderemos a brazas torcidas. Definiremos además una versión local: la p-nilpotencia a derecha e izquierda donde p es un primo que divide al orden de la braza torcida.

Comencemos comentando algunos hechos generales.

Notación 2.0.1. *Dado un conjunto finito X, $\pi(X)$ denotará al conjunto de divisores primos del cardinal de X.*

Dados dos subconjuntos X e Y de una braza torcida A, escribiremos $X * Y$ para referirnos al subgrupo de $(A, +)$ generado por los elementos de la forma $x * y$ con $x \in X$ e $y \in Y$.

Lema 2.0.2. *Sea A una braza torcida finita de tipo nilpotente y $p \in \pi(A)$. Todos los p-subgrupos de Sylow de $(A, +)$ son ideales a izquierda de A.*

Demostración. Véase, por ejemplo [22, Lemma 4.10]. □

El lema 2.0.2 deja de ser válido si quitamos la hipótesis de tipo nilpotente. En el ejemplo 1.2.3, la braza torcida G tiene grupo multiplicativo isomorfo al grupo cíclico C_6 y grupo aditivo isomorfo al grupo simétrico $\mathbb{S}_3$ que no es nilpotente. En este caso, los 2-subgrupos de Sylow de $(G, +)$ no son ideales de la braza torcida G.

Definición 2.0.3. Si G es un grupo finito y $p \in \pi(G)$, escribimos $|G| = p^k m$ con m no divisible por p. Un *p'-subgrupo de Hall* de G es un subgrupo de orden m.

Lema 2.0.4. *Sea A una braza torcida de tipo nilpotente. Para cada $p \in \pi(A)$ consideramos*

$$A_{p'} = \sum_{q \in \pi(A) \setminus \{p\}} A_q,$$

el p'-subgrupo de Hall de $(A,+)$ que es la suma directa de los q-subgrupos de Sylow de $(A,+)$ denotados por A_q. Entonces, $A_{p'}$ es un subgrupo normal de $(A,+)$ y es un ideal a izquierda de A.

Demostración. Como $(A,+)$ es nilpotente, $A_{p'}$ es un subgrupo normal de $(A,+)$. Más aún, $A_{p'}$ es un ideal a izquierda de A gracias al lema 2.0.2 y al hecho de que la suma de ideales a izquierda es un ideal a izquierda. □

2.1. Nilpotencia a derecha e izquierda de una braza torcida

A continuación resumiremos dos tipos de nilpotencia que pueden definirse sobre brazas torcidas. En lo que sigue exploraremos estas nociones y sus generalizaciones.

Una sucesión de ideales de una braza torcida que resulta ser de mucha utilidad se define recursivamente como

$$\begin{cases} A^{(1)} = A \\ A^{(n+1)} = A^{(n)} * A, \quad \text{para cada } n \geq 1. \end{cases}$$

Decimos que una braza torcida A es *nilpotente a derecha* si $A^{(n)} = 0$ para algún $n \geq 1$.

Para estudiar la nilpotencia a derecha de brazas torcidas de tipo abeliano y la retractabilidad de soluciones involutivas, Rump definió, en [55], una sucesión creciente de ideales:

$$0 = \operatorname{Soc}_0(A) \subseteq \operatorname{Soc}_1(A) \subseteq \cdots \subseteq \operatorname{Soc}_n(A) \subseteq \ldots \tag{2.1}$$

En el contexto de brazas torcidas, la sucesión (2.1) se define recursivamente de la siguiente forma: $\operatorname{Soc}_0(A) = 0$ y para cada $n \geq 1$, $\operatorname{Soc}_{n+1}(A)$ es el ideal de A que contiene a $\operatorname{Soc}_n(A)$ que satisface que $\pi(\operatorname{Soc}_{n+1}(A))) = \operatorname{Soc}(\pi(A))$ donde denotamos por $\pi : A \to A/\operatorname{Soc}_n(A)$ a la proyección canónica. Es decir que $\operatorname{Soc}_{n+1}(A)$ es el ideal de A que cumple la igualdad:

$$\operatorname{Soc}_{n+1}(A)/\operatorname{Soc}_n(A) = \operatorname{Soc}\left(A/\operatorname{Soc}_n(A)\right)$$

Para una braza torcida A y dos elementos $x, y \in A$, escribimos

$$[x,y]_+ = x + y - x - y$$

para referirnos al conmutador aditivo de x e y. La demostración del siguiente lema es directa.

Lema 2.1.1. *Si A es una braza torcida, entonces*

$$\operatorname{Soc}_{n+1}(A) = \{x \in A : x * a \in \operatorname{Soc}_n(A) \ y \ [x,a]_+ \in \operatorname{Soc}_n(A) \text{ para todo } a \in A\}.$$

Lema 2.1.2. *Si A es una braza torcida de tipo nilpotente. Entonces, A es nilpotente a derecha si y solo si $A = \mathrm{Soc}_n(A)$ para algún $n \in \mathbb{N}$.*

Demostración. Se sigue de [22, Lemma 2.15, Lemma 2.16]. □

Para dar una noción de nilpotencia a izquierda de una braza torcida A necesitamos la siguiente sucesión de ideales a izquierda, definida recursivamente:

$$\begin{cases} A^1 = A \\ A^{n+1} = A * A^n, \quad \text{para cada } n \geq 1. \end{cases}$$

Decimos que A es *nilpotente a izquierda* si $A^n = 0$ para algún $n \geq 1$. Para distintos resultados sobre brazas torcidas nilpotentes a izquierda, véanse [18, 22, 50, 55, 60, 61, 63].

2.2. Grupos de Bieberbach

En esta sección utilizaremos nociones básicas sobre la teoría de *grupos de Bieberbach* que hemos extraído de [65]. A continuación resumimos las nociones estrictamente necesarias para nuestro objetivo.

Un grupo G se dice que es un *grupo de Bieberbach de dimensión n* si se trata de un grupo sin torsión que contiene una subgrupo normal abeliano A de índice finito, isomorfo a $\mathbb{Z}^n$ y tal que $C_G(A) = A$ donde $C_G(A)$ denota al centralizador de A, es decir

$$C_G(A) = \{g \in G : ga = ag \text{ para todo } a \in A\}.$$

En consecuencia, tenemos una sucesión exacta corta

$$0 \to A \to G \xrightarrow{p} P \to 1$$

donde $P = G/A$ es un grupo finito y $p : G \to P$ es el epimorfismo canónico. Construiremos a continuación una acción de P sobre A. Dado un elemento $y \in P$, elegimos $x \in G$ tal que $p(x) = y$ y definimos la acción $h : P \to \mathrm{Aut}(A)$ dada por $h(y)(a) := xax^{-1}$. Esta acción resulta estar bien definida y ser fiel gracias a la condición $C_G(A) = A$. Cabe aclarar que h no es más que la acción inducida por la acción de conjugación de G sobre A.

En la teoría de grupos de Bieberbach, a P se le conoce como el *grupo de holonomía* de G, la función h es la *representación de holonomía* de G y A es el *subgrupo de traslaciones* de G.

Podemos pensar al grupo G como un subgrupo discreto del grupo de isometrías de un espacio euclídeo de dimensión n. Es decir, $G \subseteq \mathcal{O}_n(\mathbb{R}) \ltimes \mathbb{R}^n$ donde $\mathcal{O}_n(\mathbb{R})$ denota al grupo de transformaciones ortogonales sobre $\mathbb{R}^n$. Desde este punto de vista, el subgrupo de traslaciones A es $G \cap \mathbb{R}^n$, véase [32, p. 533].

En [39, Theorem 1.6], Gateva-Ivanova y Van den Bergh demostraron que si (X, r) es una solución involutiva finita entonces su grupo de estructura $G(X, r)$ es un grupo de Bieberbach de dimensión $|X|$.

Apoyados en este resultado y siguiendo algunas ideas de [31] mostraremos explícitamente una representación fiel del grupo de estructura de una solución involutiva finita que nos permita pensar a estos grupos como subgrupos de $\mathcal{O}_n(\mathbb{R}) \ltimes \mathbb{R}^n$. Más aún, daremos una representación para el grupo de holonomía.

Teorema 2.2.1. *Sea (X, r) una solución involutiva finita de tamaño n. Entonces existe un morfismo inyectivo de grupos $G(X, r) \to \mathcal{O}_n(\mathbb{R}) \ltimes \mathbb{R}^n$. En particular, $G(X, r)$ es isomorfo a un subgrupo de $\mathbf{GL}(n+1, \mathbb{Z})$.*

Demostración. Denotemos por $\mathbb{S}_X$ al grupo de permutaciones de los elementos de X y por $\mathbb{Z}^X$ al grupo abeliano libre generado por $\{t_x : x \in X\}$.

Sea $M_X = \mathbb{S}_X \ltimes \mathbb{Z}^X$ el producto semidirecto asociado a la acción de $\mathbb{S}_X$ sobre $\mathbb{Z}^X$. Por las proposiciones 2.3 y 2.4 de [31], la función $X \to M_X$, $x \mapsto (\sigma_x, t_x)$ se extiende a un morfismo inyectivo de grupos $G(X, r) \to M_X$.

Si pensamos a $\mathbb{S}_X$ como las matrices de permutaciones, podemos ver a $\mathbb{S}_X$ como un subgrupo de $\mathcal{O}_n(\mathbb{Z}) \subseteq \mathcal{O}_n(\mathbb{R})$. Luego, dado que $\mathbb{Z}^X \simeq \mathbb{Z}^n \subseteq \mathbb{R}^n$, se sigue que M_X es isomorfo a un subgrupo del producto semidirecto $\mathcal{O}_n(\mathbb{R}) \ltimes \mathbb{R}^n$.

La segunda parte del enunciado se deduce del hecho de que la multiplicación en $\mathcal{O}_n(\mathbb{R}) \ltimes \mathbb{R}^n$ está dada por

$$(A, a)(B, b) = (AB, a + Ab),$$

donde identificamos cada $(A, a) \in M_X$ con la matriz $\left(\begin{smallmatrix} A & a \\ 0 & 1 \end{smallmatrix}\right) \in \mathbf{GL}(n+1, \mathbb{Z})$. □

Notemos que bajo esta identificación podemos pensar en el zócalo de $G(X, r)$ como el subgrupo de traslaciones, es decir el conjunto de elementos de $\mathcal{O}_n(\mathbb{R}) \ltimes \mathbb{R}^n$ de la forma $(I, a) \in M_X \subseteq \mathbf{GL}(n+1, \mathbb{Z})$. Más aún, veamos que

$$C_{G(X,r)}\Big(\operatorname{Soc}\Big(G(X, r)\Big)\Big) = \operatorname{Soc}\Big(G(X, r)\Big).$$

Como $\operatorname{Soc}(G(X, r))$ es un subgrupo abeliano, claramente

$$\operatorname{Soc}\Big(G(X, r)\Big) \subseteq C_{G(X,r)}\Big(\operatorname{Soc}\Big(G(X, r)\Big)\Big).$$

Para cada $(I, x) \in \operatorname{Soc}(G(X, r))$ y $(A, a) \in C_{G(X,r)}(\operatorname{Soc}(G(X, r)))$ tenemos

$$(A, a)(I, x)(A^{-1}, -A^{-1}a) = (I, Ax) = (I, x),$$

luego $Ax = x$ para todos los elementos de $\{x \in \mathbb{R}^n : (I, x) \in \operatorname{Soc}(G(X, r))\}$. Debido al primer teorema de Bieberbach (véase [65, Theorem 2.1]) este conjunto genera $\mathbb{R}^n$, por lo cual $(A, a) \in C_{G(X,r)}(\operatorname{Soc}(G(X, r)))$ si y solo si $A = I$. En consecuencia, los únicos elementos del grupo que centralizan al zócalo son precisamente los elementos del zócalo.

Por [39, Theorem 1.6] sabemos que el grupo de estructura de una solución involutiva finita es un grupo de Bieberbach. Como corolario directo del primer teorema de Bieberbach, el zócalo es el subgrupo de traslaciones y es un subgrupo sin torsión que además es maximal con la propiedad de ser normal y abeliano de índice finito.

Luego, el grupo de holonomía se corresponde exactamente con el grupo de permutaciones de la solución. La representación de holonomía h es la acción de conjugación de $G(X,r)$ sobre el zócalo que se puede factorizar mediante una representación fiel. Resumimos este resultado en el siguiente teorema que utilizaremos más adelante.

Teorema 2.2.2. *Sea (X,r) una solución involutiva finita. Entonces $G(X,r)$ es un grupo de Bieberbach con grupo de holonomía isomorfo a $\mathcal{G}(X,r)$.*

2.2.1. Aplicaciones a la EYB

Las soluciones por multipermutaciones están estrechamente relacionadas a los grupos ordenables a izquierda. Un grupo $(G,\cdot)$ se dice *ordenable a izquierda* si se puede definir una relación de orden total $<$ en G tal que si $a<b$ entonces $c\cdot a<c\cdot b$ cualesquiera sean $a,b,c\in G$.

Jespers y Okniński demostraron en [43, Proposition 4.2] que el grupo de estructura de una multipermutación involutiva finita es *poly-*$\mathbb{Z}$ (es decir, que admite una serie subnormal de subgrupos tales que los cocientes sucesivos son isomorfos a $\mathbb{Z}$) y entonces resulta ordenable a izquierda.

Independientemente, en [25, Theorem 2] Chouraqui, estudiando ordenabilidad a izquierda de grupos de estructura de soluciones involutivas, demostró el mismo resultado. En [12, Theorem 2.1] se demuestra que una solución involutiva finita es multipermutación si y sólo si su grupo de estructura es ordenable a izquierda.

Decimos que un grupo G es *difuso* si para todo subconjunto finito A de G existe un elemento $a\in A$ tal que cualquiera sea $g\in G, g\neq 1$ se cumple que $ga\notin A$ o $g^{-1}a\notin A$.

En [48, Theorem 7.12] se demuestra que el grupo de estructura de una solución involutiva finita y no degenerada es ordenable a izquierda si y sólo si es difuso. Recopilamos estos hechos conocidos en el siguiente teorema.

Teorema 2.2.3. *Sea (X,r) una solución involutiva finita. Son equivalentes:*

1. *(X,r) es una solución por multipermutación;*
2. *$G(X,r)$ es poly-$\mathbb{Z}$;*
3. *$G(X,r)$ es ordenable a izquierda;*
4. *$G(X,r)$ es difuso.*

Como aplicación del teorema 2.2.3 se puede demostrar el siguiente caso particular de un teorema probado por Cedó, Jespers y Okniński en [20] y por Cameron y Gateva–Ivanova en [37].

Corolario 2.2.4. *Sea (X,r) una solución involutiva finita. Si $\mathcal{G}(X,r)$ es un grupo cíclico entonces (X,r) es una multipermutación.*

Demostración. Como X es finito, el grupo $G(X,r)$ es finitamente generado. Resulta ser libre de torsión y además $\operatorname{Soc}(G(X,r))$ es un subgrupo abeliano normal tal que

$$G(X,r)/\operatorname{Soc}(G(X,r)) \simeq \mathcal{G}(X,r)$$

es cíclico. Esto implica que $G(X,r)$ es ordenable a izquierda por [53, Lemma 13.3.1] y entonces (X,r) es una multipermutación gracias al teorema 2.2.3. □

Utilizando propiedades de grupos difusos podemos obtener una generalización del corolario 2.2.4:

Teorema 2.2.5. *Sea (X,r) una solución involutiva finita tal que todos los subgrupos de Sylow de $\mathcal{G}(X,r)$ son cíclicos. Entonces (X,r) es una multipermutación.*

Demostración. Por el teorema 2.2.2, el grupo de estructura $G(X,r)$ es un grupo de Bieberbach con grupo de holonomía isomorfo a $\mathcal{G}(X,r)$. Como todos los p-subgrupos de Sylow de $\mathcal{G}(X,r)$ son cíclicos, todos los grupos de Bieberbach con grupo de holonomía isomorfos a $\mathcal{G}(X,r)$ son difusos por [45, Theorem 3.5]. En particular, $G(X,r)$ es difuso y el resultado se sigue por el teorema 2.2.3. □

El recíproco del teorema 2.2.5 no es cierto como podemos ver en el siguiente ejemplo.

Ejemplo 2.2.6. Sea $X = \{1,2,3,4\}$ y $r(x,y) = (\varphi_x(y), \varphi_y(x))$, donde

$$\varphi_1 = \varphi_2 = \mathrm{id}, \quad \varphi_3 = (34), \quad \varphi_4 = (12)(34).$$

Entonces (X,r) es una multipermutación involutiva. Además, se puede comprobar fácilmente que $\mathcal{G}(X,r) \simeq C_2 \times C_2$.

Veamos ahora lo que ocurre al aplicar el teorema 2.2.5 a brazas finitas. El siguiente resultado de Cedó, Jespers y Okniński se encuentra implícito en [10].

Lema 2.2.7. *Sea A una braza finita. Entonces (A, r_A) es una solución involutiva tal que $\mathcal{G}(A, r_A) \simeq A/\operatorname{Soc}(A)$.*

Demostración. Basta ver que $A/\operatorname{Soc}(A) \simeq \mathcal{G}(A, r_A)$. El grupo de permutaciones $\mathcal{G}(A, r_A) = \{\lambda_a : a \in A\}$ es una braza tal que su grupo aditivo está dado por $\lambda_a + \lambda_b = \lambda_a \lambda_{\lambda_a^{-1}(b)}$ para $a, b \in A$.

Esto implica que la función $\lambda\colon (A,\circ) \to \operatorname{Aut}(A,+)$, $a \mapsto \lambda_a$ es un morfismo de brazas y entonces

$$A/\operatorname{Soc}(A) \simeq \lambda(A) = \{\lambda_a : a \in A\} = \mathcal{G}(A, r_A)$$

por el primer teorema de isomorfismo. □

Aplicamos ahora el teorema 2.2.5 para obtener un resultado sobre la estructura de las brazas.

Teorema 2.2.8. *Sea A una braza finita. Si todos los subgrupos de Sylow del grupo multiplicativo de A son cíclicos entonces A es nilpotente a derecha.*

Demostración. Si $(A, \circ)$ tienen todos sus subgrupos de Sylow cíclicos, entonces $(A/\operatorname{Soc}(A), \circ)$ tiene la misma propiedad. Por el lema 2.2.7, $A/\operatorname{Soc}(A)$ y $\mathcal{G}(A, r_A)$ son brazas isomorfas. En particular, $\mathcal{G}(A, r_A)$ tiene todos sus subgrupos de Sylow cíclicos. Luego, (A, r_A) es una multipermutación por el teorema 2.2.5. La conclusión se deduce de [18, Proposition 6]. □

El siguiente corolario del teorema 2.2.8 es inmediato.

Corolario 2.2.9. *Sea A una braza finita no trivial. Si todos los subgrupos de Sylow del grupo multiplicativo son cíclicos, entonces A no es simple.*

Teniendo en cuenta los resultados anteriores, es natural preguntarse si los teoremas 2.2.5 y 2.2.8 siguen siendo válidos bajo la hipótesis de que los subgrupos de Sylow sean abelianos. El siguiente ejemplo nos muestra que la hipótesis no se puede relajar.

Ejemplo 2.2.10. Existe una única braza simple de tamaño 72, véanse [21, Remark 4.5] y [47, Proposition 4.3]. El grupo multiplicativo de esta braza es isomorfo a $\mathbb{A}_4 \times \mathbb{S}_3$ (donde $\mathbb{A}_4$ denota al grupo alternado de 4 letras) y entonces todos sus subgrupos de Sylow son abelianos. Como el zócalo de esta braza es trivial, la solución canónica a la **EYB** asociada a esta braza no puede ser una multipermutación (más aún, es irretractable).

El corolario 2.5.14 nos dará una generalización del teorema 2.2.8 para el caso de soluciones no involutivas utilizando las técnicas de [50] y brazas torcidas de tipo nilpotente.

Ejemplo 2.2.11. Sea $G = \{g_j : j \in \mathbb{Z}/8\mathbb{Z}\}$. Las operaciones

$$g_i + g_j = g_{i+(-1)^i j}, \quad g_i \circ g_j = g_{i+j}$$

le dan a G estructura de braza torcida con grupo multiplicativo isomorfo al grupo cíclico C_8 de 8 elementos y grupo aditivo nilpotente (y no abeliano) isomorfo al grupo diedral $\mathbb{D}_8$ de ocho elementos. Es fácil comprobar que G es nilpotente a derecha.

2.3. Grupos con la propiedad de producto único

Estudiaremos a continuación la propiedad del producto único en grupos de estructura de soluciones involutivas. Para ello, primero recordemos la definición de la propiedad. Decimos que un grupo G tiene la *propiedad del producto único* si dados dos subconjuntos A y B de G no vacíos cualesquiera, existe un elemento $x \in G$ que se escribe de forma única como $x = ab$ con $a \in A$ y $b \in B$. Para más detalles sobre la propiedad de producto único, recomendamos consultar [53].

n	1	2	3	4	5	6	7	8
soluciones	1	2	5	23	88	595	3456	34530
no multipermutaciones	1	0	0	2	4	41	161	2375

Tabla 2.1: Cantidad de soluciones involutivas.

Resulta natural preguntarnos si el grupo de estructura $G(X,r)$ tiene la propiedad del producto único, véase por ejemplo [48, Section 8]. De hecho, si (X,r) es una multipermutación, entonces $G(X,r)$ tiene la propiedad del producto único puesto que $G(X,r)$ es ordenable a izquierda.

En [31], Etingof, Schedler y Soloviev construyeron todas las soluciones involutivas de tamaño menor o igual a 8. Hay 38700 soluciones[1] de las cuales solo 2583 resultan no ser multipermutaciones, véase la Tabla 2.1.

Nuestro objetivo es determinar si los grupos de estructura de soluciones involutivas que no son multipermutaciones resultan no tener la propiedad de producto único. Comenzamos con la siguiente observación hecha por Jespers y Okniński:

Proposición 2.3.1. *Sea $X = \{1,2,3,4\}$ y $r(x,y) = (\sigma_x(y), \tau_y(x))$ la solución irretractable e involutiva dada por*

$$\begin{aligned} &\sigma_1 = (34), && \sigma_2 = (1324), && \sigma_3 = (1423), && \sigma_4 = (12),\\ &\tau_1 = (24), && \tau_2 = (1432), && \tau_3 = (1234), && \tau_4 = (13). \end{aligned}$$

El grupo de estructura $G(X,r)$ con generadores x_1, x_2, x_3, x_4 y relaciones

$$\begin{aligned} &x_1x_2 = x_2x_4, && x_1x_3 = x_4x_2, && x_1x_4 = x_3^2,\\ &x_2x_1 = x_3x_4, && x_2^2 = x_4x_1, && x_3x_1 = x_4x_3. \end{aligned}$$

no tiene la propiedad del producto único.

Demostración. Véase [44, Example 8.2.14]. □

En la demostración de la proposición 2.3.1, Jespers y Okniński encuentran un subgrupo del grupo de estructura isomorfo a un subgrupo de Promislow. Esta idea la explotaremos en la Sección 2.4.

Proposición 2.3.2. *Sea $X = \{1,2,3,4\}$ y $r(x,y) = (\sigma_x(y), \tau_y(x))$ la solución involutiva e irretractable dada por*

$$\begin{aligned} &\sigma_1 = (12), && \sigma_2 = (1324), && \sigma_3 = (34), && \sigma_4 = (1423),\\ &\tau_1 = (14), && \tau_2 = (1243), && \tau_3 = (23), && \tau_4 = (1342). \end{aligned}$$

Entonces, el grupo de estructura $G(X,r)$ con generadores x_1, x_2, x_3, x_4 y relaciones

$$\begin{aligned} &x_1^2 = x_2x_4, && x_1x_3 = x_3x_1, && x_1x_4 = x_4x_3,\\ &x_2x_1 = x_3x_2, && x_2^2 = x_4^2, && x_3^2 = x_4x_2. \end{aligned}$$

no tiene la propiedad del producto único.

[1] Este número incluye una pequeña corrección al conteo original hecha en [5].

Demostración. Sean $x = x_1x_2^{-1}$ y $y = x_1x_3^{-1}$. Consideremos el subconjunto

$$S = \{x^2y, y^2x, xyx^{-1}, (y^2x)^{-1}, (xy)^{-2}, y, (xy)^2x, (xy)^2, (xyx)^{-1}, yxy, y^{-1}, x, xyx, x^{-1}\}. \quad (2.2)$$

Para demostrar que $G(X, r)$ no tiene la propiead del producto único alcanza con probar que todos los elementos $s \in S^2 = \{s_1s_2 : s_1, s_2 \in S\}$ admiten al menos dos escrituras diferentes de la forma $s = ab = uv$ con $a, b, u, v \in S$. Para verificar este hecho, utilizamos la representación fiel $G \to \mathbf{GL}(5, \mathbb{Z})$ que nos da el teorema 2.2.1,

$$x_1 \mapsto \begin{pmatrix} 0&1&0&0&1\\1&0&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{pmatrix}, \qquad x_2 \mapsto \begin{pmatrix} 0&0&0&1&0\\0&0&1&0&1\\1&0&0&0&0\\0&1&0&0&0\\0&0&0&0&1\end{pmatrix},$$

$$x_3 \mapsto \begin{pmatrix} 1&0&0&0&0\\0&1&0&0&0\\0&0&0&1&1\\0&0&1&0&0\\0&0&0&0&1\end{pmatrix}, \qquad x_4 \mapsto \begin{pmatrix} 0&0&1&0&0\\0&0&0&1&0\\0&1&0&0&0\\1&0&0&0&1\\0&0&0&0&1\end{pmatrix}.$$

Con la ayuda de esta representación, podemos calcular todos los productos de la forma s_1s_2 para todo par de elementos $s_1, s_2 \in S$. Por simple inspección, verificamos que cada elemento de S^2 admiten al menos dos escrituras como las buscadas. □

Sobre las últimas dos proposiciones, podemos sacar algunas observaciones y conclusiones.

Observación 2.3.3. Las soluciones de las proposiciones 2.3.1 y 2.3.2 son las únicas soluciones involutivas de tamaño 4 que no son multipermutaciones. Podemos afirmar entonces que los grupos de estructura de soluciones involutivas de tamaño 4 que no son multipermutaciones, no tienen la propiedad de producto único.

Observación 2.3.4. El conjunto (2.2) aparece en el trabajo de Promislow, véase [54].

Observación 2.3.5. La técnica que utilizamos para demostrar la proposición 2.3.2 se puede utilizar para demostrar la proposición 2.3.1.

Proposición 2.3.6. *Sea $G(X, r)$ el grupo de estructura de una solución involutiva de tamaño menor o igual a 7 que no es una multipermutación. Luego, $G(X, r)$ no tiene la propiedad de producto único.*

Demostración. La demostración es un análisis caso por caso usando la misma técnica que utilizamos en la demostración de la proposición 2.3.2 y la lista de soluciones de tamaño ≤ 7 de [31]. En muchos casos, los elementos x e y que forman el subconjunto (2.2) fueron encontrados mediante una búsqueda aleatoria. □

En principio, el argumento utilizado para demostrar las proposiciones 2.3.2, 2.3.6 y 2.3.7 se puede utilizar para el caso de soluciones de tamaño ocho. La siguiente solución aparece en [67] como un contraejemplo a una conjetura de Gateva–Ivanova relacionada a la retractabilidad de soluciones libres de cuadrados, véase [36, 2.28(1)].

Proposición 2.3.7. *Sea* $X = \{1, \dots, 8\}$ *y* $r(x, y) = (\varphi_x(y), \varphi_y(x))$ *la solución involutiva e irretractable dada por*

$$\begin{array}{llll} \varphi_1 = (78), & \varphi_2 = (56), & \varphi_3 = (25)(46)(78), & \varphi_4 = (17)(38)(56), \\ \varphi_5 = (24), & \varphi_6 = (17)(24)(38), & \varphi_7 = (13), & \varphi_8 = (13)(25)(46). \end{array}$$

Entonces, $G(X, r)$ *no tiene la propiedad de producto único.*

Demostración. Sean $x = x_4 x_2^{-1} x_1 x_3^{-1}$ e $y = x_1 x_2^{-1} x_3 x_1^{-1} x_4 x_1^{-1}$ (estos elementos fueron hallados mediante una búsqueda aleatoria).

La representación fiel $G(X, r) \to \mathbf{GL}(9, \mathbb{Z})$ del teorema 2.2.1 nos permite utilizar el conjunto (2.2) para probar que $G(X, r)$ no tiene la propiedad del producto único. □

Hay soluciones de tamaño ocho para las cuales nuestra técnica no parece funcionar. Por ejemplo:

Ejemplo 2.3.8. Sea $X = \{1, \dots, 8\}$ y $r(x, y) = (\sigma_x(y), \tau_y(x))$, donde

$$\begin{array}{ll} \sigma_1 = \sigma_2 = (3745), & \tau_1 = \tau_2 = (3648), \\ \sigma_3 = \sigma_4 = (1826), & \tau_3 = \tau_4 = (1527), \\ \sigma_5 = \sigma_7 = (13872465), & \tau_5 = \tau_7 = (16542873), \\ \sigma_6 = \sigma_8 = (17842563), & \tau_6 = \tau_8 = (13562478). \end{array}$$

Luego, (X, r) es una solución involutiva que se retrae a la solución de la proposición 2.3.1. En particular, (X, r) no es una multipermutación.

La Tabla 2.2 muestra cuatro soluciones involutivas cuyos retractos son la solución de la proposición 2.3.1 y para las cuales no parece funcionar nuestra técnica; la solución del ejemplo 2.3.8 es la primera entrada de la Tabla 2.2. Por otro lado, en la Tabla 2.3 se exhiben cuatro soluciones involutivas cuyos retractos son la solución de la proposición 2.3.2 y para las cuales no parece funcionar nuestra técnica. No sabemos si los grupos de estructura de las soluciones de ambas tablas tienen o no la propiedad de producto único.

2.4. Cómo hallar subgrupos de Promislow

En esta sección explicaremos la teoría general que utilizaremos para encontrar subgrupos isomorfos al grupo de Promislow en un cierto grupo de Bieberbach. El grupo de Promislow fue el primer ejemplo de un grupo sin torsión que no posee la propiedad de producto único, véase [54].

Lema 2.4.1. *Sea* P *el grupo de Promislow*

$$\langle x, y \mid x^{-1} y^2 x = y^{-2}, y^{-1} x^2 y = x^{-2} \rangle.$$

Luego, $A = \langle x^2, y^2, (xy)^2 \rangle$ *es un subgrupo normal abeliano libre de* P *de rango* 3 *con* P/A *isomorfo al grupo de Klein de* 4 *elementos. Más aún,* P *es un grupo ordenable a izquierda sin torsión.*

x	σ_x	τ_x	σ_x	τ_x
1	(3745)	(3648)	(3745)(68)	(3648)(57)
2	(3745)	(3648)	(3745)(68)	(3648)(57)
3	(1826)	(1527)	(1826)(57)	(1527)(68)
4	(1826)	(1527)	(1826)(57)	(1527)(68)
5	(13872465)	(16542873)	(1465)(2387)	(1654)(2873)
6	(17842563)	(13562478)	(1784)(2563)	(1478)(2356)
7	(13872465)	(16542873)	(1465)(2387)	(1654)(2873)
8	(17842563)	(13562478)	(1784)(2563)	(1478)(2356)
1	(12)(4675)	(12)(3685)	(12)(35)(4867)	(12)(3857)(46)
2	(12)(4675)	(12)(3685)	(12)(35)(4867)	(12)(3857)(46)
3	(1435)(2786)	(1578)(2643)	(16582437)	(17652843)
4	(1587)(2634)	(1345)(2876)	(17562834)	(15682347)
5	(1823)(56)	(1724)(56)	(16582437)	(17652843)
6	(1823)(56)	(1724)(56)	(17562834)	(15682347)
7	(1587)(2634)	(1345)(2876)	(1325)(46)(78)	(1426)(35)(78)
8	(1435)(2786)	(1578)(2643)	(1325)(46)(78)	(1426)(35)(78)

Tabla 2.2: Soluciones de tamaño cuatro que se retraen a la solución de la proposición 2.3.1.

x	σ_x	τ_x	σ_x	τ_x
1	(12)(78)	(14)(67)	(12)(35)(46)(78)	(14)(28)(35)(67)
2	(1584)(2673)	(1265)(3784)	(1324)(5867)	(1243)(5786)
3	(34)(56)	(23)(58)	(17)(28)(34)(56)	(17)(23)(46)(58)
4	(1485)(2376)	(1562)(3487)	(1423)(5768)	(1342)(5687)
5	(34)(56)	(23)(58)	(17)(28)(34)(56)	(17)(23)(46)(58)
6	(1485)(2376)	(1562)(3487)	(1423)(5768)	(1342)(5687)
7	(12)(78)	(14)(67)	(12)(35)(46)(78)	(14)(28)(35)(67)
8	(1584)(2673)	(1265)(3784)	(1324)(5867)	(1243)(5786)
1	(13687542)	(13867524)	(1652)	(1854)
2	(17)(2583)(46)	(1278)(35)(46)	(17645328)	(12835647)
3	(18657243)	(16857423)	(3874)	(2367)
4	(1476)(28)(35)	(17)(28)(3456)	(14635827)	(17825346)
5	(18657243)	(16857423)	(1652)	(1854)
6	(1476)(28)(35)	(17)(28)(3456)	(17645328)	(12835647)
7	(13687542)	(13867524)	(3874)	(2367)
8	(17)(2583)(46)	(1278)(35)(46)	(14635827)	(17825346)

Tabla 2.3: Soluciones de tamaño cuatro que se retraen a la solución de la proposición 2.3.2.

Demostración. Véase por ejemplo [53, Lemma 13.3.3]. □

Sea $\Gamma \subseteq \mathbf{GL}(n,\mathbb{Z}) \ltimes \mathbb{Z}^n$ un grupo de Bieberbach definido por la siguiente sucesión exacta corta

$$0 \longrightarrow L \longrightarrow \Gamma \xrightarrow{\pi} \Gamma/L \longrightarrow 0. \tag{2.3}$$

Estamos tomando $L \subseteq \mathbb{Z}^n$ de manera que $\{I\} \times L$ es el subgrupo abeliano normal maximal de Γ, donde I representa la matriz identidad en $\mathbf{GL}(n,\mathbb{Z})$ y π es el morfismo canónico, es decir $\pi(A,a) = A$.

Diremos que dos elementos x, y de un grupo G satisfacen (P) si y sólo si

$$x^2y = yx^{-2} \quad \text{and} \quad y^2x = xy^{-2} \tag{P}$$

se cumple en G.

Lema 2.4.2. *Sean $\alpha = (A,a)$ y $\beta = (B,b)$ elementos de Γ que generan un subgrupo isomorfo a P. Luego, se cumple que:*

1. *$A \neq I$ y $B \neq I$;*
2. *A y B satisfacen* (P).

Demostración. Tenemos la siguiente sucesión exacta corta:

$$0 \longrightarrow \langle \alpha^2, \beta^2, (\alpha\beta)^2 \rangle \longrightarrow P \longrightarrow C_2^2 \longrightarrow 0.$$

Para ver que $A \neq I$ y $B \neq I$, supongamos que $A = I$. Sea $k \in \mathbb{N}$ tal que $\beta^{2k} = (I, b')$; esto puede hacerse puesto que $\pi(\beta) = B$ pertenece a un grupo finito. Entonces

$$\beta^{-2k} = \alpha^{-1}\beta^{2k}\alpha = (I,-a)(I,b')(I,a) = (I,b') = \beta^{2k},$$

que contradice el hecho de que Γ es un grupo sin torsión.

Para ver que A y B satisfacen (P) sólo debemos notar que $\pi(\alpha) = A$ y $\pi(\beta) = B$ y que α, β satisfacen (P). □

Utilizaremos dos polinomios de Laurent:

$$P_1(X,Y) = 1 + X + YX^{-1} + YX^{-2}, \qquad P_2(X,Y) = -1 + X^2.$$

Lema 2.4.3. *Sean G un grupo y $A, B \in G$ dos elementos que satisfacen* (P). *Sean (A,v) y (B,w) un par de elementos de Γ que se proyectan a A y B respectivamente. Si*

$$\begin{bmatrix} P_1(A,B) & P_2(A,B) \\ P_2(B,A) & P_1(B,A) \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = - \begin{bmatrix} P_1(A,B) & P_2(A,B) \\ P_2(B,A) & P_1(B,A) \end{bmatrix} \begin{bmatrix} v \\ w \end{bmatrix}$$

tiene una solución entera $x, y \in L$, entonces

$$\alpha = (A, x+v) \quad y \quad \beta = (B, y+w)$$

satisfacen (P).

Demostración. Veamos que $\alpha^2\beta = \beta\alpha^{-2}$. Por la hipótesis, $A^2B = BA^{-2}$. Luego, identificando α y β como matrices, tenemos que $\alpha^2\beta = \beta\alpha^{-2}$ es equivalente a $P_1(A,B)(x+v) + P_2(A,B)(y+w) = 0$, lo cual es cierto por hipótesis. De forma análoga, $\beta^2\alpha = \alpha\beta^{-2}$. □

Proposición 2.4.4. *Sea* Γ *un grupo definido por una sucesión exacta corta como* (2.3). *Sean* $\alpha, \beta \in \Gamma$ *tales que* $\pi(\alpha) \neq I$, $\pi(\beta) \neq I$. *Si* α *y* β *satisfacen* (P), *entonces generan un subgrupo de* Γ *isomorfo a* P.

Demostración. Sean $P = \langle \alpha, \beta \rangle$, $L_P = \langle a, b, c \rangle$ donde $a = \alpha^2, b = \beta^2, c = (\alpha\beta)^2$. Entonces P es un grupo de Bieberbach con la siguiente sucesión exacta corta

$$0 \longrightarrow L_P \longrightarrow P \longrightarrow C_2^2 \longrightarrow 0.$$

L_P es un subgrupo abeliano de Γ, por lo tanto es abeliano libre y es un subgrupo abeliano maximal normal de P. Basta ver que L_P tiene rango 3. Sean n_a, n_b, n_c enteros tales que $a^{n_a}b^{n_b}c^{n_c} = 1$. Conjugando por α obtenemos $a^{n_a}b^{-n_b}c^{-n_c} = 1 = a^{n_a}b^{n_b}c^{n_c}$ y por lo tanto $b^{2n_b}c^{2n_c} = 1$. Conjugando nuevamente por β obtenemos $c^{4n_c} = 1$. Como Γ es un grupo sin torsión, tenemos que $n_a = n_b = n_c = 0$. □

Observación 2.4.5. Los cálculos propuestos en la proposición anterior se pueden realizar fácilmente utilizando la representación de [33, Lemma 1] que incluimos aquí por completitud:

$$\left\langle \alpha = \begin{pmatrix} 1 & 0 & 0 & 1/2 \\ 0 & -1 & 0 & 1/2 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \beta = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1/2 \\ 0 & 0 & -1 & 1/2 \\ 0 & 0 & 0 & 1 \end{pmatrix} \right\rangle \subseteq \mathbf{GL}(4, \mathbb{Q}).$$

A continuación mostramos un algoritmo para encontrar subgrupos (de un grupo de Bieberbach) que son isomorfos al grupo de Promislow:

Algoritmo 2.4.6. Sea $\Gamma \subseteq \mathbf{GL}(n, \mathbb{Z}) \ltimes \mathbb{Z}^n$ un grupo de Bieberbach definido por la siguiente sucesión exacta corta

$$0 \longrightarrow L \longrightarrow \Gamma \xrightarrow{\pi} \Gamma/L \longrightarrow 0,$$

donde $L \subseteq \mathbb{Z}^n$ fue elegido de forma que $\{I\} \times L$ es el subgrupo maximal normal abeliano de Γ y π es el morfimo canónico. Por comodidad, llamaremos G al grupo Γ/L

1. Buscar entre todos los pares $A, B \in G \setminus \{1\}$ aquellos que satisfacen (P).
2. Determinar preimágenes $(A, v) \in \pi^{-1}(A)$ y $(B, w) \in \pi^{-1}(B)$.
3. Verificar si el sistema lineal del lema 2.4.3 tiene soluciones enteras. Por la proposición 2.4.4, la existencia de tales soluciones es equivalente a la existencia de un subgrupo isomorfo a P.

Como aplicación, el siguiente teorema mejora el resultado de la proposición 2.3.6.

Teorema 2.4.7. *Sea $G(X,r)$ el grupo de estructura de una solución involutiva que no es una multipermutación de tamaño ≤ 8. Entonces $G(X,r)$ contiene un subgrupo isomorfo al subgrupo de Promislow si y sólo si (X,r) no es isomorfo a alguna de las soluciones de las tablas 2.2 y 2.3.*

Demostración. La demostración es un análisis caso por caso utilizando el Algoritmo 2.4.6 y la lista de soluciones involutivas de [31]. □

2.5. p-nilpotencia a derecha en brazas torcidas

Sea A una braza torcida a izquierda. Dados dos subconjuntos X e Y de A definimos recursivamente $R_0(X,Y) = X$ y $R_{n+1}(X,Y)$ como el subgrupo aditivo generado por $R_n(X,Y) * Y$ y $[R_n(X,Y),Y]_+$ para $n \geq 0$.

Lema 2.5.1. *Sea I un ideal de una braza torcida A. Entonces $R_{n+1}(I,A) \subseteq R_n(I,A)$ para todo $n \geq 0$.*

Demostración. La demotración es por inducción en n. El caso base $n = 0$ es trivial ya que I es un ideal de A. Supongamos que el enunciado es cierto para algún valor $n \geq 0$. Por hipótesis inductiva $R_n(I,A) * A \subseteq R_{n-1}(I,A) * A \subseteq R_n(I,A)$ y

$$[R_n(I,A),A]_+ \subseteq [R_{n-1}(I,A),A]_+ \subseteq R_n(I,A),$$

por lo cual se sigue que $R_{n+1}(I,A) \subseteq R_n(I,A)$. □

Proposición 2.5.2. *Sea I un ideal de una braza torcida A. Entonces cada uno de los $R_{n+1}(I,A)$ es un ideal de A.*

Demostración. La demostración es por inducción en n. El caso $n = 0$ es consecuencia de que I es un ideal de A. Supongamos que el resultado es cierto para algún $n \geq 0$. Primero, probemos que $R_{n+1}(I,A)$ es un subgrupo normal de $(A,+)$. Sean $a,b \in A$ y $x \in R_n(I,A)$. Luego

$$a + x * b - a = -x * a + x * (a+b) \in R_{n+1}(I,A),$$

por definición. Además

$$a+(x+b-x-b)-a = (a+x-a)+(a+b-a)-(a+x-a)-(a+b-a) \in R_{n+1}(I,A)$$

por hipótesis inductiva, en consecuencia $R_{n+1}(I,A)$ es un subgrupo normal de $(A,+)$.

Veamos ahora que

$$\lambda_a(R_{n+1}(I,A)) \subseteq R_{n+1}(I,A) \tag{2.4}$$

para todo $a \in A$. Usando la hipótesis inductiva y que cada $\lambda_a \in \mathrm{Aut}(A,+)$,

$$\lambda_a(x * b) = (a \circ x \circ a') * \lambda_a(b) \in R_{n+1}(I,B)$$

y

$$\lambda_a([R_n(I,A),A]_+) \subseteq [\lambda_a(R_n(I,A)),\lambda_a(A)]_+ \\ \subseteq [R_n(I,A),A]_+ \subseteq R_{n+1}(I,A),$$

se sigue la igualdad (2.4).

Como $R_{n+1}(I,A) \subseteq R_n(I,A)$ por lema 2.5.1,

$$R_{n+1}(I,A) * A \subseteq R_n(I,A) * A \subseteq R_{n+1}(I,A).$$

La afirmación se sigue de [22, Lemma 1.9].

□

Lema 2.5.3. *Sea A una braza torcida, X un subconjunto de A y $n, m \in \mathbb{N}$. Entonces $R_m(X,A) \subseteq \mathrm{Soc}_n(A)$ si y solo si $X \subseteq \mathrm{Soc}_{m+n}(A)$.*

Demostración. Procedamos por inducción en m. El caso $m = 0$ es trivial. Asumamos que el resultado es válido para algún $m \geq 0$. Notemos que $R_{m+1}(X,A) \subseteq \mathrm{Soc}_n(A)$ es equivalente a $R_m(X,A) * A \subseteq \mathrm{Soc}_n(A)$ y $[R_m(X,A),A]_+ \subseteq \mathrm{Soc}_n(A)$. Por lema 2.1.1, esto es equivalente a $R_m(X,A) \subseteq \mathrm{Soc}_{n+1}(A)$, que a su vez es equivalente a $X \subseteq \mathrm{Soc}_{m+n+1}(A)$ por hipótesis inductiva. □

Lema 2.5.4. *Una braza torcida A de tipo nilpotente es nilpotente a derecha si y sólo si $R_n(A,A) = 0$ para algún $n \in \mathbb{N}$.*

Demostración. Por lema 2.5.3, $R_n(A,A) = 0$ si y sólo si $A = \mathrm{Soc}_n(A)$. Por lema 2.1.2, esto último es equivalente a la nilpotencia a derecha de A. □

Recordemos que un grupo finito G es *p-nilpotente* si existe un p'-subgrupo de Hall normal de G. Se puede ver que un tal subgrupo es característico en G. Siguiendo las ideas de [50], definimos la propiedad de p-nilpotencia a derecha para brazas torcidas de tipo nilpotente:

Definición 2.5.5. Sea p un número primo. Una braza torcida finita A de tipo nilpotente es *p-nilpotente a derecha* si existe $n \geq 1$ tal que $R_n(A_p,A) = 0$, donde A_p es el p-subgrupo de Sylow de $(A,+)$.

Proposición 2.5.6. *Sea A una braza torcida finita de tipo nilpotente y $p \in \pi(A)$. Entonces $A_p \subseteq \mathrm{Soc}_n(A)$ para algún $n \geq 1$ si y sólo si A es p-nilpotente a derecha.*

Demostración. Por lema 2.5.3, $R_n(A_p,A) = 0$ si y sólo si $A_p \subseteq \mathrm{Soc}_n(A)$. □

Proposición 2.5.7. *Una braza torcida finita A de tipo nilpotente es nilpotente a derecha si y sólo si A es p-nilpotente a derecha para todo $p \in \pi(A)$.*

Demostración. Supongamos que A es nilpotente a derecha. Por lema 2.1.2, existe $n \in \mathbb{N}$ tal que $A_p \subseteq A = \mathrm{Soc}_n(A)$ para todo $p \in \pi(A)$. Luego, la afirmación se sigue de la proposición 2.5.6.

Supongamos que A es p-nilpotente a derecha para todo $p \in \pi(A)$. En consecuencia para cada $p \in \pi(A)$ existe $n(p) \in \mathbb{N}$ tal que $A_p \subseteq \mathrm{Soc}_{n(p)}(A)$. Sea $n = \max\{n(p) : p \in \pi(A)\}$. Entonces $A_p \subseteq \mathrm{Soc}_n(A)$ para todo $p \in \pi(A)$. Como $\mathrm{Soc}_n(A)$ es un ideal de A y A es de tipo nilpotente, $A = \oplus_{p\in\pi(A)} A_p \subseteq \mathrm{Soc}_n(A)$. Luego A es nilpotente a derecha por lema 2.1.2. □

En [50], Meng, Ballester–Bolinches y Romero demostraron el siguiente teorema para el caso de brazas torcidas de tipo abeliano que nosotros extendemos a brazas torcidas de tipo nilpotente.

Teorema 2.5.8. *Sea A una braza torcida finita de tipo nilpotente. Si $(A, \circ)$ tiene un p-subgrupo de Sylow normal abeliano para algún $p \in \pi(A)$, entonces A es p-nilpotente a derecha.*

Nuestra demostración es muy similar a la de [50]. Haremos uso de los siguientes lemas:

Lema 2.5.9. *Sea A una braza torcida finita de tipo nilpotente. Si $(A, \circ)$ tiene un p-subgrupo de Sylow normal para algún $p \in \pi(A)$ entonces A_p es un ideal de A.*

Demostración. Como el grupo $(A, +)$ es nilpotente, existe un único p-subgrupo de Sylow normal A_p de $(A, +)$. Por lema 2.0.2, A_p es un ideal a izquierda de A. Entonces A_p es un p-subgrupo de Sylow de $(A, \circ)$, normal por hipótesis y en consecuencia A_p es un ideal de A. □

Lema 2.5.10. *Sea A una braza torcida finita de tipo nilpotente. Si $(A, \circ)$ tiene un p-subgrupo de Sylow normal para algún $p \in \pi(A)$ entonces* $\mathrm{Soc}(A_p) = \mathrm{Soc}(A) \cap A_p$. *En particular,* $\mathrm{Soc}(A_p)$ *es un ideal de A.*

Demostración. Por lema 2.5.9, A_p es un ideal de A.

Claramente $\mathrm{Soc}(A_p) \supseteq \mathrm{Soc}(A) \cap A_p$ por lo que solo tenemos que probar que $\mathrm{Soc}(A_p) \subseteq \mathrm{Soc}(A) \cap A_p$. Si $a \in \mathrm{Soc}(A_p)$, entonces $a \in Z(A_p, +)$ y $a * b = 0$ para todo $b \in A_p$. Sea $c \in A$ y escribamos $c = x + y$, donde $x \in A_p$ y $y \in A_{p'}$. Como

$$a * c = a * (x + y) = \underbrace{a * x}_{=0} + x + a * y - x = x + a * y - x \in A_p \cap A_{p'} = 0$$

y $a \in Z(A, +)$, el lema queda demostrado. □

Ahora estamos en condiciones de demostrar el teorema 2.5.8.

Demostración. Supongamos que el teorema no es válido y sea A un contraejemplo de tamaño minimal. Podemos asumir que A no es trivial, es decir $\mathrm{Soc}(A) \neq A$. Por lema 2.5.9, A_p es un ideal de A.

Como $\lambda_a \in \mathrm{Aut}(A_p, +)$ y $\lambda_a(Z(A_p, +)) \subseteq Z(A_p, +)$ tenemos que $Z(A_p, +)$ es un ideal a izquierda de A_p.

Por lema 2.5.10, $\mathrm{Soc}(A_p)$ es un ideal de A. Más aún, como $(A_p, \circ)$ es abeliano,

$$\begin{aligned}
\mathrm{Soc}(A_p) &= \{a \in A_p : a * b = 0 \text{ para todo } b \in A_p\} \cap Z(A_p, +) \\
&= \{a \in A_p : a \circ b = a + b \text{ para todo } b \in A_p\} \cap Z(A_p, +) \\
&= \{a \in A_p : b \circ a = b + a \text{ para todo } b \in A_p\} \cap Z(A_p, +) \\
&= \mathrm{Fix}(A_p) \cap Z(A_p, +).
\end{aligned}$$

Como $|A_p| = p^m$ para algún $m \geq 1$, la braza torcida A_p es nilpotente a izquierda por [22, Proposition 4.4] y ademaś $Z(A_p, +)$ es un subgrupo no nulo de $(A_p, +)$. Entonces $\mathrm{Soc}(A_p) = \mathrm{Fix}(A_p) \cap Z(A_p, +) \neq 0$ por [22, Proposition 2.26].

En particular, $0 \neq \mathrm{Soc}(A_p) \subseteq \mathrm{Soc}(A)$. Por lema 2.5.10, $I = \mathrm{Soc}(A_p)$ es un ideal no trivial de A. Entonces A/I es una braza torcida de tipo nilpotente con $0 < |A/I| < |A|$. La minimalidad de $|A|$ implica que A/I es p-nilpotente a derecha. Luego, $R_n(A_p/I, A/I) = 0$ para algún n. Es decir que $R_n(A_p, A) \subseteq I \subseteq \mathrm{Soc}(A)$. Ahora, por lema 2.5.3, $R_{n+1}(A_p, A) = 0$. Luego A es p-nilpotente a derecha, lo que contradice la hipótesis. □

Recordemos que un grupo G tiene la *propiedad de la torre de Sylow* si existe una serie normal $1 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$ tal que cada cociente G_i/G_{i-1} es isomorfo a un subgrupo de Sylow de G. Recordemos también que un *A–grupo* es un grupo finito cuyos subgrupos de Sylow son abelianos.

Corolario 2.5.11. *Sea A una braza torcida de tipo nilpotente. Supongamos que $(A, \circ)$ tiene la propiedad de la torre de Sylow y que todos los subgrupos de Sylow de $(A, \circ)$ son abelianos. Entonces A es nilpotente a derecha.*

Demostración. Supongamos que el resultado no es válido y sea A un contraejemplo de tamaño mínimo. Como $(A, \circ)$ tiene la propiedad de la torre de Sylow, existe un p-subgrupo de Sylow normal A_p de $(A, \circ)$. Entonces A_p es un ideal no nulo de A y se puede ver que

$$0 \neq \mathrm{Soc}(A_p) = \mathrm{Soc}(A) \cap A_p \subseteq \mathrm{Soc}(A).$$

El grupo $(A/\mathrm{Soc}(A), \circ)$ tiene subgrupos de Sylow abelianos y tiene la propiedad de la torre de Sylow. Como A es una braza torcida no trivial, $0 < |A/\mathrm{Soc}(A)| < |A|$, y entonces $A/\mathrm{Soc}(A)$ es nilpotente a derecha por la minimalidad de $|A|$. Por [22, Proposition 2.17], A es nilpotente a derecha, una contradicción. □

Hay ejemplos de brazas torcidas de tipo abeliano que son nilpotentes a derecha donde el grupo multiplicativo contiene un subgrupo de Sylow no abeliano o bien no tiene la propiedad de la torre de Sylow:

Ejemplo 2.5.12. El grupo abeliano $\mathbb{Z}/8$ con la operación $a \circ b = a + 3^a b$ es una braza torcida de tipo abeliano nilpotente a derecha con grupo multiplicativo isomorfo al grupo de cuaterniones. Este ejemplo aparece en [7].

Ejemplo 2.5.13. Sea $G = \mathbb{A}_4 \times \mathbb{S}_3$. Cada subgrupo de Sylow de G es abeliano, por lo cual se sigue de [21, Theorem 2.2] y [19, Theorem 2.1] que existe una braza torcida de tipo abeliano con grupo multiplicativo isomorfo al grupo G. El grupo G no tiene la propiedad de la torre de Sylow. Un rastreo por la base de datos de brazas torcidas de tipo abeliano de [41] muestra que hay sólo 4 con grupo multiplicativo isomorfo a G, todas ellas con grupo aditivo isomorfo a $C_6 \times C_6 \times C_2$. Sin embargo, sólo una de ellas no es nilpotente a derecha.

Como corolario, obtenemos una generalización del teorema 2.2.8:

Corolario 2.5.14. *Sea A una braza torcida finita de tipo nilpotente. Si todos los subgrupos de Sylow del grupo multiplicativo de A son cíclicos entonces A es nilpotente a derecha.*

Demostración. Como todos los subgrupos de Sylow de $(A, \circ)$ son cíclicos, el grupo $(A, \circ)$ es superresoluble y entonces tiene la propiedad de la torre de Sylow. Luego, la afirmación se sigue del corolario 2.5.11. □

2.6. p-nilpotencia a izquierda de brazas torcidas

Sea A una braza torcida. Dados dos subconjuntos X e Y de A, definimos recursivamente la sucesión $L_0(X, Y) = Y$ y $L_{n+1}(X, Y) = X * L_n(X, Y)$ para $n \geq 0$.

Definición 2.6.1. Sea p un número primo. Una braza torcida finita A de tipo nilpotente se dice que es *p-nilpotente a izquierda* si existe $n \geq 1$ para el cual $L_n(A, A_p) = 0$, donde A_p es el p-subgrupo de Sylow de $(A, +)$.

Lema 2.6.2. *Sea A una braza torcida tal que su grupo aditivo es un producto directo de ideales a izquierda B y C. Entonces $A * (B + C) = A * B + A * C$. Más aún, si $A = \oplus_{i=1}^{n} B_i$ donde los B_i son ideales a izquierda, entonces*

$$A * \sum_{i=1}^{n} B_i = \sum_{i=1}^{n} A * B_i.$$

Demostración. Sean $a \in A$, $b \in B$ y $c \in C$. Luego,

$$a * (b + c) = a * b + b + a * c - b = a * b + a * c$$

se satisface cualesquiera sean $a \in A$, $b \in B$ y $c \in C$. La segunda parte se sigue por inducción. □

Proposición 2.6.3. *Sea A una braza torcida finita de tipo nilpotente. Entonces A es nilpotente a izquierda si y sólo si A es p-nilpotente a izquierda para todo $p \in \pi(A)$.*

Demostración. Para cada $p \in \pi(A)$ existe $n(p) \in \mathbb{N}$ tal que $L_{n(p)}(A, A_p) = 0$. Sea $n = \max\{n(p) : p \in \pi(A)\}$. Luego, $L_n(A, A_p) = 0$ para todo $p \in \pi(A)$. Como A es de tipo nilpotente, el grupo $(A, +)$ es isomorfo a la suma directa de A_p para $p \in \pi(A)$. Luego, por el lema 2.6.2 tenemos que

$$L_n(A, A) = \sum_{p \in \pi(A)} L_n(A, A_p) = 0.$$

La otra implicación es trivial. □

El siguiente teorema fue probado por Meng, Ballester–Bolinches y Romero para brazas torcidas de tipo abeliano (véase [50]). Veamos que podemos extenderlo al caso de brazas torcidas de tipo nilpotente.

Teorema 2.6.4. *Sea A una braza torcida finita de tipo nilpotente. Son equivalentes:*

1. *A es p-nilpotente a izquierda;*
2. *$A_{p'} * A_p = 0$;*
3. *El grupo $(A, \circ)$ es p-nilpotente.*

Demostración. Veamos primero que (1) implica (2). Como A es p-nilpotente a izquierda, existe $n \in \mathbb{N}$ tal que $L_n(A_{p'}, A_p) \subseteq L_n(A, A_p) = 0$. Como $(A'_p, \circ)$ actúa por automorfismos en $(A_p, +)$ y la acción es coprima, se sigue por [42, Lemma 4.29] que

$$L_1(A_{p'}, A_p) = A_{p'} * A_p = A_{p'} * (A_{p'} * A_p) = L_2(A_{p'}, A_p).$$

Por inducción, vemos que $A_{p'} * A_p = L_n(A'_p, A_p) = 0$.

Veamos ahora que (2) implica (3). Basta ver que $(A_{p'}, \circ)$ es un subgrupo normal de $(A, \circ)$. Por el lema 2.6.2,

$$A_{p'} * A = A_{p'} * (A_p + A_{p'}) = (A_{p'} * A_p) + (A_{p'} * A_{p'}) \subseteq A_{p'}.$$

puesto que A'_p es un ideal a izquierda de A y $A_{p'} * A_p = 0$. Luego, $A_{p'}$ es un ideal de A por Lema 2.0.4 y [22, Lemma 1.9]. En particular, $(A_{p'}, \circ)$ es un subgrupo normal de $(A, \circ)$.

Por último, veamos que (3) implica (1). Debemos ver que $L_n(A_p, A_p) = 0$ para algún n. Como $(A, \circ)$ es p-nilpotente, existe un p-complemento normal que es un subgrupo característico de $(A, \circ)$. Este grupo es $A_{p'}$ y en consecuencia $A_{p'}$ resulta ser un ideal de A. Luego $A_{p'} * A_p \subseteq A_{p'} \cap A_p = 0$. Veamos que $L_n(A, A_p) = L_n(A_p, A_p)$ para todo $n \geq 0$. El caso $n = 0$ es trivial. Supongamos que es válido para algún valor de $n \geq 0$. Por hipótesis inductiva,

$$L_{n+1}(A, A_p) = A * L_n(A, A_p) = A * L_n(A_p, A_p).$$

Luego basta ver que $A * L_n(A_p, A_p) \subseteq A_p * L_n(A_p, A_p)$. Sean $a \in A$ y $b \in L_n(A_p, A_p)$. Escribamos $a = x \circ y$ con $x \in A_p$ e $y \in A_{p'}$. Luego

$$a * b = (x \circ y) * b = x * (y * b) + y * b + x * b = x * b \in A_p * L_n(A_p, A_p)$$

puesto que $A_{p'} * A_p = 0$.

La braza torcida A_p es nilpotente a izquierda por [22, Proposition 4.4], por lo cual existe $n \in \mathbb{N}$ tal que $L_n(A_p, A_p) = 0$. □

El siguiente teorema fue probado por Smoktunowicz para brazas torcidas de tipo abeliano, véase [61, Theorem 1.1]. Para brazas torcidas, hay una demostración en [22, Theorem 4.8].

Teorema 2.6.5. *Sea A una braza torcida de tipo nilpotente. Luego A es nilpotente a izquierda si y sólo si el grupo multiplicativo de A es nilpotente.*

Demostración. Como fue observado en [50], la proposición 2.6.3 y el teorema 2.6.4 prueban el teorema. □

Parte 3

Clasificación de brazas torcidas de orden pq y p^2q

Capítulo 3

Brazas torcidas de orden pq

En principio, el problema de hallar soluciones no degeneradas de la **EYB** se puede reducir al problema de clasificación de brazas torcidas. En efecto, dada una solución involutiva no degenerada el grupo de permutaciones $\mathcal{G}(X,r) = \{\sigma_x : x \in X\}$ tiene una estructura canónica de braza. En [10] Bachiller, Cedó y Jespers construyen todas las soluciones involutivas no degeneradas de la **EYB** con una estructura de braza prefijada sobre el grupo de permutaciones. En [9], Bachiller generaliza esta construcción considerando un grupo de permutaciones asociado a una solución no degenerada que resulta tener una estructura natural de braza torcida, [9, Theorem 3.11]. En consecuencia, con ese trabajo, el problema de clasificación de todas las soluciones no degeneradas se reduce al problema de clasificación de todas las brazas torcidas.

Recientemente, han habido muchos avances en el problema de clasificación de brazas (torcidas). Las brazas con grupo aditivo cíclico y las de tamaño p^2q para p, q números primos con $q > p+1$ fueron clasificadas en [56, 59] y [29], respectivamente. En [7], Bachiller resolvió el problema para brazas de orden p^2 y p^3 con p un número primo y en [51], Nejabati Zenouz completó la clasificación de brazas torcidas de orden p^3. En [52], Nejabati Zenouz incluye los grupos de automorfismos de brazas torcidas de orden p^3 de tipo Heisenberg. En [6], se enumeran las brazas torcidas de orden libre de cuadrados. En el presente capítulo resolveremos el siguiente problema.

Problema. *[68, Problem 2.15] Sean p y q números primos distintos. Construir todas las brazas torcidas de orden pq salvo isomorfismos.*

Nuestra clasificación se basa en el algoritmo de construcción de brazas torcidas desarrollado en [41]. En efecto, el algoritmo permite construir todas las brazas torcidas con grupo aditivo A a partir de subgrupos regulares del holomorfo $\mathrm{Hol}(A) = A \rtimes \mathrm{Aut}(A)$. Las clases de isomorfismo de brazas torcidas se obtienen como las órbitas de la acción dada por conjugación inducida por el grupo de automorfismos de A sobre $\mathrm{Hol}(A)$, [41, Section 4].

La conexión entre brazas torcidas, subgrupos regulares y extensiones Hopf–Galois fue observada por primera vez por Bachiller en [8, Remark 2.8]. Para más detalles acerca de esa conexión, recomendamos recurrir al Apéndice de [63].

En [15], Byott señala un aproximación a las extensiones Hopf–Galois desde la teoría de grupos para poder enumerar las extensiones sobre un grupo dado. en particular, las extensiones Hopf–Galois de grado pq donde $p > q$ son números primos fueron investigadas en [16] a partir de una descripción explícita de subgrupos regulares.

Utilizaremos esa descripción como primer paso para clasificar brazas torcidas de tamaño pq. La conclusión de este capítulo se puede resumir en el siguiente teorema.

Teorema. *Sean $p > q$ números primos. Si $p \not\equiv 1 \pmod{q}$, existe una única braza torcida de tamaño pq, la trivial. Si $p \equiv 1 \pmod{q}$, la siguiente es una lista completa de las $2q+2$ brazas torcidas de orden pq, salvo isomorfismo, donde g es un elemento fijo de $\mathbb{Z}_p$ de orden multiplicativo q:*

- *Grupo aditivo $\mathbb{Z}_p \times \mathbb{Z}_q$:*

$$\binom{n}{m} + \binom{s}{t} = \binom{n+s}{m+t};$$

  (i) la braza trivial sobre $\mathbb{Z}_p \times \mathbb{Z}_q$;

  (ii) la bi-braza torcida $(A, +, \circ)$ donde

$$\binom{n}{m} \circ \binom{s}{t} = \binom{n + g^m s}{m+t}.$$

- *Grupo aditivo $\mathbb{Z}_p \rtimes_g \mathbb{Z}_q$:*

$$\binom{n}{m} + \binom{s}{t} = \binom{n + g^m s}{m+t};$$

  (i) la braza torcida trivial sobre $\mathbb{Z}_p \rtimes_g \mathbb{Z}_q$;

  (ii) la braza torcida $(A, +, \circ)$ con

$$\binom{n}{m} \circ \binom{s}{t} = \binom{g^t n + g^m s}{m+t};$$

  (iii) las bi-brazas torcidas $A_\gamma = (A, +, \circ)$ para $1 < \gamma \leq q$ donde

$$\binom{n}{m} \circ \binom{s}{t} = \binom{n + (g^\gamma)^m s}{m+t};$$

  (iv) las brazas torcidas $A_\mu = (A, +, \circ)$ for $1 < \mu \leq q$ donde

$$\binom{n}{m} \circ \binom{s}{t} = \binom{g^t n + (g^\mu)^m s}{m+t}.$$

Observación 3.0.1. Nuestros resultados coinciden con la fórmula hallada por Byott y Alabdali en [6, Section 7.2] para enumerar brazas torcidas de tamaño libre de cuadrados.

3.1. Preliminares

A continuación mostramos una forma de construir bi-brazas torcidas sobre productos semidirectos de grupos. La primera parte es un caso especial de [51, Proposition 4.6.12] pero incluimos una demostración por completitud.

Proposición 3.1.1. *Sean A un grupo cualquiera y B un grupo abeliano. Consideremos $\eta, \rho : B \longrightarrow \mathrm{Aut}(A)$ morfismos de grupos. Si $[Im(\rho), Im(\eta)] = 1$ entonces $G_{\eta,\rho} = (G, +, \circ)$ donde $(G, +) = A \rtimes_\eta B$ y $(G, \circ) = A \rtimes_\rho B$ es una bi-braza torcida con $A \times \{0\} \leq \ker \lambda$.*

Demostración. Notemos por ρ_x y η_x las imágenes de ρ y η para cada $x \in B$. Luego

$$\begin{aligned}(x, s) \circ ((y, t) + (z, u)) &= (x, s) \circ (y\eta_t(z), t + u) \\ &= (x\rho_s(y)\rho_s(\eta_t(z)), s + t + u)\end{aligned}$$

y por otro lado

$$\begin{aligned}((x, s) \circ (y, t)) - (x, s) + ((x, s) \circ (z, u)) = \\ &= (x\rho_s(y), s + t) + (\eta_{-s}(x)^{-1}, -s) + (x\rho_s(z), s + u) \\ &= (x\rho_s(y)\eta_t(x)^{-1}, t) + (x\rho_s(z), s + u) \\ &= (x\rho_s(y)\eta_t(x)^{-1}\eta_t(x)\eta_t(\rho_s(z)), t + s + u) \\ &= (x\rho_s(y)\eta_t(\rho_s(z)), t + s + u)\end{aligned}$$

cualesquiera sean $x, y, z \in A$ y $s, t, u \in B$. Como η_t y ρ_s conmutan entonces $(A, +, \circ)$ es una braza torcida. El mismo argumento muestra que $(A, \circ, +)$ es, a su vez, una braza torcida. Más aún,

$$\begin{aligned}\lambda_{(x,s)}(y, t) &= -(x, s) + (x, s) \circ (y, t) = (\eta_{-s}(x)^{-1}, -s) + (x\rho_s(y), t + s) \\ &= (\eta_{-s}(x)^{-1}\eta_{-s}(x)\eta_{-s}(\rho_s(y)), t) \\ &= (\eta_{-s}(\rho_s(y)), t). \qquad (3.1)\end{aligned}$$

para todos $x, y \in A$ y $s, t \in B$. Entonces $A \times \{0\} \leq \ker \lambda$. □

La proposición 3.1.1 se puede aplicar a grupos cíclicos ya que sus grupos de automorfismos son abelianos.

Corolario 3.1.2. *Sean A un grupo cíclico y B un grupo abeliano, $(G, +) = A \rtimes_\eta B$ y $(G, \circ) = A \rtimes_\rho B$. Entonces $G_{\eta,\rho}$ es una bi-braza torcida y $A \times \{0\} \leq \ker \lambda$.*

El *holomorfo* de un grupo $(A, +)$ es el producto semidirecto $A \rtimes \mathrm{Aut}(A)$ donde la operación está dada por

$$(a, f)(b, g) = (a + f(b), fg),$$

para todos $a, b \in A$ y $f, g \in \mathrm{Aut}(A)$.

Denotamos por $\pi_1 : \mathrm{Hol}(A) \to A$ y $\pi_2 : \mathrm{Hol}(A) \to \mathrm{Aut}(A)$ las funciones canónicas. Notemos que $\mathrm{Hol}(A)$ actúa sobre A mediante $(a, f)(b) = a + f(b)$, para todos $(a, f) \in \mathrm{Hol}(A)$ y $b \in A$. Luego $\mathrm{Hol}(A)$ es un grupo de permutaciones de A.

Recordemos que un grupo de permutaciones N de un conjunto X se dice *regular* si, dados $x, y \in X$, existe un único $g \in N$ tal que $g(x) = y$.

Gracias a [41], sabemos que dado un grupo $(A, +)$ (no necesariamente abeliano) tenemos una correspondencia biyectiva entre clases de isomorfismos de brazas torcidas $(A, +, \circ)$ y las órbitas de los subgrupos regulares de $\mathrm{Hol}(A, +)$ bajo la acción de conjugación por $\mathrm{Aut}(A, +)$ (identificado con el subgrupo $\{1\} \times \mathrm{Aut}(A) \leq \mathrm{Hol}(A, +)$). Si G es un subgrupo regular de $\mathrm{Hol}(A, +)$, entonces es fácil verificar que la función $\pi_1|_G : G \to A$ es biyectiva.

Teorema 3.1.3. *[41, Theorem 4.2, Proposition 4.3] Sea $(A, +)$ un grupo. Si $\circ$ es una operación tal que $(A, +, \circ)$ es una braza torcida, entonces $\{(a, \lambda_a) : a \in A\}$ es un subgrupo regular de $\mathrm{Hol}(A, +)$. Recíprocamente, si G es un subgrupo regular de $\mathrm{Hol}(A, +)$, entonces A es una braza torcida con*

$$a \circ b = a + f(b)$$

donde $(\pi_1|_G)^{-1}(a) = (a, f) \in G$ y $(A, \circ) \cong G$.

Más aún, las clases de isomorfismo de brazas torcidas sobre A están en correspondencia biyectiva con las órbitas de de subgrupos regulares de $\mathrm{Hol}(A)$ bajo la acción de $\mathrm{Aut}(A)$ por conjugación.

En [16] aparece una descripción explícita de todos los subgrupos regulares de $\mathrm{Hol}(A)$ para grupos de orden pq, donde p, q son números primos distintos. En consecuencia, podemos construir todas las brazas torcidas con grupo aditivo isomorfo a A buscando representantes de las órbitas de subgrupos regulares bajo la acción de conjugación por $\mathrm{Aut}(A)$ en $\mathrm{Hol}(A)$ y además, podemos dar una fórmula explícita para las operaciones de tales brazas torcidas utilizando el teorema 3.1.3. Respetando la notación de [16], denotamos por $e'(G, A, m)$ la cantidad de subgrupos regulares de $\mathrm{Hol}(A)$ isomorfos a un grupo dado G tal que su imagen por π_2 tiene tamaño m.

Observación 3.1.4. Sean $(A, +)$ un grupo y G un subgrupo regular de $\mathrm{Hol}(A)$. De acuerdo con el teorema 3.1.3, $(A, +, \circ)$ donde

$$a \circ b = a + \pi_2((\pi_1|_G)^{-1}(a))(b)$$

para todos $a, b \in A$ es una braza torcida. En otras palabras, $\lambda_a = \pi_2(\pi_1|_G^{-1}(a))$ y entonces $|\ker \lambda| = \frac{|G|}{|\pi_2(G)|}$.

Dado que en este capítulo utilizaremos la lista de representantes de subgrupos regulares de $\mathrm{Hol}(A)$ provista por [16], no analizaremos en profundidad las técnicas necesarias para llegar a una lista exhaustiva de subgrupos. En la sección 4.1.1 y subsiguientes del capítulo 4 retomaremos la construcción.

3.2. Grupos de orden pq y sus grupos de automorfismos

A continuación listaremos todos los grupos de orden pq salvo isomorfismos y describiremos explícitamente sus grupos de automorfismos. Consideraremos por comodidad, $p > q$ dos números primos.

Si $p \not\equiv 1 \pmod{q}$, el único grupo de orden pq es el grupo cíclico; para referirnos a él utilizaremos la siguiente presentación:

$$C = \langle \sigma, \tau \,|\, \sigma^p = \tau^q = 1,\, \tau\sigma = \sigma\tau \rangle. \tag{3.2}$$

El grupo $\mathrm{Aut}(C)$ es isomorfo a $\mathbb{Z}_{p-1} \times \mathbb{Z}_{q-1}$ y utilizaremos la siguiente presentación:

$$\mathrm{Aut}(C) = \langle \phi, \psi \mid \phi^{p-1} = \psi^{q-1} = 1,\, \phi\psi = \psi\phi \rangle \tag{3.3}$$

donde los morfismos ϕ y ψ se definen como

$$\begin{aligned} \phi(\sigma) &= \sigma^n, & \psi(\sigma) &= \sigma, \\ \phi(\tau) &= \tau, & \psi(\tau) &= \tau^m, \end{aligned}$$

considerando que n tiene orden multiplicativo $p-1$ módulo p y m tiene orden multiplicativo $q-1$ módulo q.

Si $p \equiv 1 \pmod{q}$, tenemos además un único grupo no abeliano que presentaremos como

$$M = \langle \sigma, \tau \,|\, \sigma^p = \tau^q = 1,\, \tau\sigma = \sigma^g\tau \rangle \cong \mathbb{Z}_p \rtimes_g \mathbb{Z}_q \tag{3.4}$$

donde g tiene orden multiplicativo q módulo p. Respetando la notación de [16], notaremos por a_0 a un número entero fijo que satisfaga

$$(g-1)a_0 \equiv 1 \pmod{p}. \tag{3.5}$$

Utilizaremos la siguiente fórmula que es bien conocida:

$$\sum_{i=0}^{r-1} g^i \equiv \frac{g^r - 1}{g-1} \equiv a_0(g^r - 1) \pmod{p} \tag{3.6}$$

para todo $r \in \mathbb{N}$.

Una descripción de los elementos de $\mathrm{Aut}(M)$ viene dada por el siguiente lema.

Lema 3.2.1. *[40, Lemma 2.3] Los automorfismos de M son*

$$\{\varphi_{i,j} \,:\, 1 \le i \le p-1,\, 0 \le j \le p-1\}$$

donde $\varphi_{i,j}(\sigma) = \sigma^i$ y $\varphi_{i,j}(\tau) = \sigma^j\tau$.

3.3. Brazas torcidas de orden pq

Recordemos que p y q son números primos con $p > q$.

3.3.1. Brazas torcidas triviales

Como ya mencionamos, una braza torcida $(A, +, \circ)$ se dice *trivial* si $a + b = a \circ b$ cualesquiera sean $a, b \in A$. Para cualquier grupo G existe una única braza torcida trivial A con $G = (A, +) = (A, \circ)$. Luego, si $p \equiv 1 \pmod{q}$, existen dos brazas torcidas triviales de tamaño pq. Por otro lado, si $p \not\equiv 1 \pmod{q}$ existe una única braza torcida de tamaño pq y es trivial. Para ver esto, recordemos que un número natural n se dice *número de Burnside* si n es coprimo con $\phi(n)$, la función de Euler.

Proposición 3.3.1. *Sean $p > q$ dos números primos tales que $p \not\equiv 1 \pmod{q}$. Existe una única braza torcida de tamaño pq (la trivial) con $(A, +) = (A, \circ) \cong \mathbb{Z}_{pq}$.*

Demostración. Si $p \not\equiv 1 \pmod{q}$, entonces pq es un número de Burnside, luego existe una única braza torcida de tamaño pq, [63, Theorem A.8]. □

3.3.2. Brazas torcidas de tipo cíclico

Vamos a concentrarnos ahora en las brazas con grupo aditivo cíclico de tamaño pq. Este caso está contenido en la clasificación dada en [56, 59] y sólo la incluimos por completitud. Por la proposición 3.3.1, podemos asumir que $p \equiv 1 \pmod{q}$ a partir de ahora.

Toda imagen no trivial de un grupo de orden pq por un morfismo a $\mathrm{Aut}(C)$ tiene tamaño q ya que $|\mathrm{Aut}(C)| = (p-1)(q-1)$ y q divide a $p-1$. Luego, sólo debemos considerar subgrupos regulares tales que su imagen por π_2 es de orden q.

Para lo que sigue, fijemos el automorfismo α en $\mathrm{Aut}(C)$ definido como:

$$\alpha(\sigma) = \sigma^g, \quad \alpha(\tau) = \tau.$$

Lema 3.3.2. *[16, Lemma 4.1] Los subgrupos regulares de* $\mathrm{Hol}(C)$ *tales que la imagen por π_2 tiene orden q son*

$$G_b = \langle \sigma, \tau^b \alpha \rangle \cong M, \tag{3.7}$$

donde $1 \leq b \leq q-1$. En particular, $e'(C, C, q) = 0$ y $e'(M, C, q) = q - 1$.

La enumeración de brazas torcidas de tipo cíclico se sigue de la enumeración de órbitas de subgrupos regulares de $\mathrm{Hol}(C)$.

Proposición 3.3.3. *Existe una única braza torcida de tipo abeliano de tamaño pq.*

Demostración. Basta ver que todos los subgrupos de $\mathrm{Hol}(C)$ que aparecen en el Lema 3.3.2 son conjugados entre sí por algún elemento de $\mathrm{Aut}(C)$. En efecto,

$$\begin{aligned} \psi^j G_b \psi^{-j} &= \langle \psi^j \sigma \psi^{-j}, \psi^j \tau^b \alpha \psi^{-j} \rangle \\ &= \langle \psi^j(\sigma), \psi^j(\tau)^b \alpha \rangle \\ &= \langle \sigma, \tau^{m^j b} \alpha \rangle \\ &= G_{m^j b}. \end{aligned}$$

Dado que m tiene orden multiplicativo $q-1$ módulo q, todos los subgrupos G_b son conjugados entre sí. □

Teorema 3.3.4. *La única braza torcida no trivial de tipo cíclico es* $(A, +, \circ)$ *donde* $(A, \circ) \cong \mathbb{Z}_p \rtimes_g \mathbb{Z}_q$*, es decir*

$$\binom{n}{m} + \binom{s}{t} = \binom{n+s}{m+t}, \qquad \binom{n}{m} \circ \binom{s}{t} = \binom{n+g^m s}{m+t}$$

con $0 \leq n, s \leq p-1$, $0 \leq m, t \leq q-1$. *En particular,* $(A, +, \circ)$ *es una bi-braza torcida.*

Demostración. Por el corolario 3.1.2, $(A, +, \circ)$ es una bi-braza torcida que cumple que $|\ker \lambda| = p$. Por la proposición 3.3.3, $(A, +, \circ)$ es la única braza torcida con esas propiedades. □

3.3.3. Brazas torcidas de tipo no abeliano

Seguimos suponiendo que p y q son números primos tales que $p \equiv 1 \pmod{q}$. Para enumerar brazas torcidas no triviales con grupo aditivo isomorfo a M debemos hallar $e'(G, M, m)$ para $m \in \{p, q, pq\}$ y $G \in \{C, M\}$.

El único subgrupo de orden pq en $\mathrm{Aut}(M)$ es el subgrupo generado por

$$\alpha = \varphi_{1,1}, \quad \beta = \varphi_{g,0} \tag{3.8}$$

con la notación del lema 3.2.1. Luego, la imagen por λ de cualquier braza torcida de tamaño pq está contenida en este subgrupo.

Lema 3.3.5. *[16, Lemma 5.1] Los subgrupos regulares de* $\mathrm{Hol}(M)$ *tales que la imagen por* π_2 *tiene orden* p *son*

$$G_c = \langle \sigma^{a_0}\alpha, \sigma^c \tau \rangle \cong C \tag{3.9}$$

con $0 \leq c \leq p-1$. *En particular,* $e'(M, M, p) = 0$ *y* $e'(C, M, p) = p$.

Teorema 3.3.6. *Existe una única braza torcida de orden* pq *con grupo aditivo* M *y* $|\ker \lambda| = q$. *Más aún, se trata de* $(A, +, \circ)$ *donde*

$$\binom{n}{m} + \binom{s}{t} = \binom{n+g^m s}{m+t}, \qquad \binom{n}{m} \circ \binom{s}{t} = \binom{g^t n + g^m s}{m+t} \tag{3.10}$$

para todo $0 \leq n, s \leq p-1$, $0 \leq m, t \leq q-1$.

Demostración. Veamos primero que todos los subgrupos de (3.9) son conjugados de G_0 por algún elemento de $\mathrm{Aut}(M)$. Sea $0 \leq c \leq p-1$ y consideremos $\eta = \varphi_{1,-c}$, luego $\eta^{-1} = \varphi_{1,c}$. Como η centraliza a $\sigma^{a_0}\alpha$, tenemos que

$$\eta G_c \eta^{-1} = \langle \eta(\sigma^{a_0})\eta\alpha\eta^{-1}, \eta(\sigma^c\tau) \rangle = \langle \sigma^{a_0}\alpha, \tau \rangle = G_0.$$

Por ende, existe una única braza torcida con las propiedades deseadas. Es inmediato ver que $(A, +, \circ)$ definida como en (3.10) es una braza torcida y que $|\ker \lambda| = q$. □

Lema 3.3.7. *[16, Lemma 5.2] Los subgrupos regulares de* $\mathrm{Hol}(M)$ *cuyas imágenes por* π_2 *tienen orden* q *son*

$$G_{a,b} = \langle \sigma, \tau^a \alpha^b \beta \rangle, \tag{3.11}$$

donde $1 \leq a \leq q-1$ *y* $0 \leq b \leq p-1$. *En particular,* $e'(M, M, q) = p(q-2)$ *y* $e'(C, M, q) = p$.

Proposición 3.3.8. *Existen* $q-1$ *brazas torcidas con grupo aditivo* M *y* $|\ker \lambda| = p$.

Demostración. Veamos que los subgrupos $G_{a,0}$ con $1 \leq a \leq q-1$ definidos como en (3.11) forman un conjunto de representantes de las órbitas. Si $b \neq 0$,

$$\varphi_{1,-ba_0} G_{a,0} \varphi_{1,-ba_0}^{-1} = \langle \sigma, (\sigma^{-ba_0}\tau)^a \alpha^b \beta \rangle = \langle \sigma, \tau^a \alpha^b \beta \rangle = G_{a,b},$$

donde hemos multiplicado al segundo generador por alguna potencia de σ para obtener la segunda igualdad. Además, usamos las identidades $\varphi_{i,j} \alpha \varphi_{i,j}^{-1} = \alpha^i$ y $\varphi_{i,j} \beta \varphi_{i,j}^{-1} = \varphi_{g,(1-g)j} = \alpha^{(1-g)j}\beta$.

El subgrupo generado por σ es invariante por la acción por conjugación de $\mathrm{Aut}(M)$. Luego, $G_{a,0}$ y $G_{b,0}$ son conjugados entre sí si y sólo si

$$\varphi_{i,j} \tau^a \beta \varphi_{i,j}^{-1} = \varphi_{i,j}(\tau)^a \varphi_{g,(1-g)j} = \sigma^{j\frac{g^a-1}{g-1}} \tau^a \varphi_{g,(1-g)j} \in G_{b,0} \tag{3.12}$$

para algún $\varphi_{i,j} \in \mathrm{Aut}(M)$. Entonces $\tau^a \varphi_{g,(1-g)j} \in G_{b,0}$ puesto que $\sigma \in G_{b,0}$ y $\pi_2(\tau^a \varphi_{g,(1-g)j}) = \varphi_{g,(1-g)j} = \beta^k$ para algún $k \in \mathbb{N}$. Por lo tanto $j = 0$, $k = 1$ y en consecuencia $\tau^a \beta \in G_{b,0}$. Dado que $\tau^b \beta \in G_{b,0}$, tenemos que $\tau^{a-b} \in \langle \sigma \rangle$ y entonces $a = b$. □

Teorema 3.3.9. *Las brazas torcidas de orden* pq *con grupo aditivo* M *y* $|\ker \lambda| = p$ *son* $A_\gamma = (A, +, \circ)$ *con* $1 < \gamma \leq q$ *donde*

$$\binom{n}{m} + \binom{s}{t} = \binom{n + g^m s}{m + t}, \qquad \binom{n}{m} \circ \binom{s}{t} = \binom{n + (g^\gamma)^m s}{m + t}, \tag{3.13}$$

para todos $0 \leq n, s \leq p-1$, $0 \leq m, t \leq q-1$. *En particular, son bi-brazas torcidas.*

Demostración. Consideremos un representante $G = G_{a,0}$ de los subgrupos regulares de $\mathrm{Hol}(M)$ para algún $1 \leq a \leq q-1$ como en (3.11). Por la observación 3.1.4, $\lambda_\sigma = \pi_2(\sigma) = 1$ y $\lambda_{\tau^a} = \pi_2(\tau^a \beta) = \beta$. Como $a \circ b = a + \lambda_a(b)$, tenemos que

$$\underbrace{\tau^a \circ \tau^a \circ \ldots \circ \tau^a}_{n} = \tau^{na}, \qquad \underbrace{\sigma \circ \sigma \circ \ldots \circ \sigma}_{n} = \sigma^n$$

para todo $n \in \mathbb{N}$. Como $\lambda : (A, \circ) \longrightarrow \mathrm{Aut}(A, +)$ es un morfismo de grupos,

$$\lambda_{\sigma^n \circ \tau^{ma}} = \lambda_{\sigma^n \tau^{ma}} = \lambda_\sigma^n \lambda_{\tau^a}^m = \beta^m$$

y entonces $\lambda_{\sigma^n \tau^m} = \beta^{\frac{m}{a}}$ para todo $0 \leq n \leq p-1$ y $0 \leq m \leq q-1$. Utilizando la notación aditiva para M y la identificación $\sigma \mapsto \binom{1}{0}$ y $\tau \mapsto \binom{0}{1}$ tenemos:

$$\binom{n}{m} \circ \binom{s}{t} = \binom{n}{m} + \beta^{\frac{m}{a}} \binom{s}{t} = \binom{n + g^{m\frac{a+1}{a}} s}{m + t}$$

para todo $0 \leq n, s \leq p-1$ y $0 \leq m, t \leq q-1$. Como $1 \leq a \leq q-1$ entonces $1 < \frac{a+1}{a} \leq q$. Dado que tanto el grupo aditivo como el multiplicativo de A_γ son productos semidirectos de grupos cíclicos, por el corolario 3.1.2, se trata de bi-brazas torcidas. □

Lema 3.3.10. *[16, Lemma 5.4] Los subgrupos regulares de* $\mathrm{Hol}(M)$ *cuyas imágenes por* π_2 *son de orden* pq *son*

$$G_{c,d} = \langle \sigma^{a_0}\alpha, \sigma^c \tau^d \beta \rangle \tag{3.14}$$

donde $d \neq 0$ *y o bien* $d \neq q-1$ *con* $0 \leq c \leq p-1$ *o bien* $d = q-1$ *y* $c = 0$. *En particular,* $e'(M, M, pq) = p(q-2)+1$.

Proposición 3.3.11. *Existen* $q-1$ *brazas torcidas con grupo aditivo* M *y* $\ker \lambda = 0$.

Demostración. Veamos que los subgrupos $G_{0,d}$ con $1 \leq d \leq q-1$ como en (3.14) forman un conjunto de representantes de las órbitas de subgrupos regulares cuyas imágenes por π_2 tienen orden pq.

Primero, conjugamos cualquier $G_{0,d}$ por un automorfismo arbitrario $\varphi_{i,j}$:

$$\begin{aligned}
\varphi_{i,j} G_{0,d} \varphi_{i,j}^{-1} &= \langle \varphi_{i,j}(\sigma^{a_0})\alpha^i, \varphi_{i,j}(\tau^d)\varphi_{g,(1-g)j} \rangle \\
&= \langle (\sigma^{a_0}\alpha)^i, (\sigma^j \tau)^d \varphi_{g,(1-g)j} \rangle \\
&= \langle \sigma^{a_0}\alpha, \sigma^{j\frac{g^d-1}{g-1}} \tau^d \varphi_{g,(1-g)j} \rangle.
\end{aligned}$$

Multiplicando por $(\sigma^{a_0}\alpha)^{(g-1)j}$ al segundo generador, obtenemos

$$\langle \sigma^{a_0}\alpha, \sigma^{j\frac{g^{d+1}-1}{g-1}} \tau^d \beta \rangle = G_{j\frac{g^{d+1}-1}{g-1}, d}.$$

Ahora, como $\frac{g^{d+1}-1}{g-1} \equiv 0 \pmod{p}$ si y sólo si $d = q-1$, tenemos que la órbita de $G_{0,q-1}$ es puntual y que la órbita de $G_{0,d}$ con $d \neq q-1$ tiene p elementos pues $j\frac{g^{d+1}-1}{g-1}$ recorre todo el intervalo desde 0 hasta p.

□

Teorema 3.3.12. *Las brazas torcidas de orden* pq *con grupo aditivo* M *y* $\ker \lambda = 0$ *son* $A_\mu = (A, +, \circ)$ *para* $1 < \mu \leq q$ *donde*

$$\binom{n}{m} + \binom{s}{t} = \binom{n + g^m s}{m+t}, \qquad \binom{n}{m} \circ \binom{s}{t} = \binom{g^t n + (g^\mu)^m s}{m+t} \tag{3.15}$$

para todos $0 \leq n, s \leq p-1$, $0 \leq m, t \leq q-1$.

Demostración. Sea $G_{0,d}$ un subgrupo regular de $\mathrm{Hol}(M)$ como en (3.14). Por la observación 3.1.4 tenemos que $\lambda_{\pi_1(x)} = \pi_2(x)$ para todo $x \in G_{0,d}$. En particular,

$$\lambda_{\sigma^{a_0}} = \alpha, \quad \lambda_{\tau^d} = \beta.$$

Como $a \circ b = a + \lambda_a(b)$, es fácil ver que

$$\underbrace{\tau^d \circ \tau^d \circ \ldots \circ \tau^d}_{n} = \tau^{nd}, \qquad \underbrace{\sigma^{a_0} \circ \sigma^{a_0} \circ \ldots \circ \sigma^{a_0}}_{n} = \sigma^{na_0}$$

para todo $n \in \mathbb{N}$. Usando el hecho de que $\lambda : (A, \circ) \longrightarrow \mathrm{Aut}(A, +)$ es un morfismo de grupos, entonces $\lambda_\sigma = \alpha^{g-1}$ y $\lambda_\tau = \beta^{d^{-1}}$. Por otro lado,

$$\begin{aligned} \sigma^n \circ \tau^m &= \sigma^n \alpha^{n(g-1)}(\tau^m) \\ &= \sigma^{n+(g^m-1)n}\tau^m \\ &= \sigma^{g^m n}\tau^m \end{aligned}$$

y entonces

$$\lambda_{\sigma^n\tau^m} = \lambda_{\sigma^{ng^{-m}}\circ\tau^m} = \lambda_{\sigma^{ng^{-m}}}\lambda_{\tau^m} = \alpha^{(g-1)ng^{-m}}\beta^{md^{-1}}$$

para todo $0 \leq n \leq p-1$, $0 \leq m \leq q-1$. Si utilizamos la notación aditiva para la operación del grupo M y usamos la identificación $\sigma \mapsto \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $\tau \mapsto \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ tenemos que

$$\begin{pmatrix} n \\ m \end{pmatrix} + \begin{pmatrix} s \\ t \end{pmatrix} = \begin{pmatrix} n + g^m s \\ m + t \end{pmatrix}, \qquad \begin{pmatrix} n \\ m \end{pmatrix} \circ \begin{pmatrix} s \\ t \end{pmatrix} = \begin{pmatrix} g^t n + g^{m\frac{d+1}{d}} s \\ m + t \end{pmatrix} \tag{3.16}$$

para todos $0 \leq n, s \leq p-1$, $0 \leq m, t \leq q-1$. Como $1 \leq d \leq q-1$ entonces $1 < \mu = \frac{d+1}{d} \leq q$ y entonces tenemos la fórmula (3.15) para la operación $\circ$. □

Capítulo 4

Brazas torcidas de orden p^2q Caso abeliano

En este capítulo comenzaremos con la enumeración y clasificación de brazas torcidas de orden p^2q donde p y q son dos números primos distintos. Dado que el objetivo es clasificar todas las brazas torcidas de este orden, comenzaremos con las brazas torcidas de tipo abeliano (es decir, *brazas* a secas). Como parte de la clasificación seremos capaces de mostrar las fórmulas que definen explícitamente a las brazas. En el próximo capítulo discutiremos la clasificación de brazas torcidas de tipo no abeliano.

La técnica básica es la que utilizamos para clasificar las brazas torcidas de orden pq en el capítulo 3 pero en esta oportunidad no contamos con una lista previa de los subgrupos regulares de $\mathrm{Hol}(A)$. Por este motivo, nuestro trabajo es mucho más extenso en este caso. El algoritmo completo de clasificación puede consultarse en [41, Section 4].

La clasificación está dividida en varios casos de acuerdo a las relaciones que se cumplen entre los números primos p y q. Comenzaremos resumiendo el método a seguir y luego procederemos con la construcción de las brazas. Como guía, resumimos en la tabla 4.1 sólo la enumeración de brazas de acuerdo con las relaciones entre p y q así como la sección en la que se trata el caso correspondiente.

En cada sección, incluimos tablas que resumen el contenido discriminando las brazas según sus grupos aditivo y multiplicativo.

Como consecuencia de este trabajo, damos una demostración alternativa de las conjeturas 6.2-6.4 de [41], demostradas previamente en [60] y [29].

En [41, Table 5.3], podemos consultar la cantidad de brazas torcidas de orden $n \leq 120$ con algunas excepciones. Gracias a una mejora computacional en el algoritmo de enumeración de brazas torcidas, en [13] podemos ver muchas tablas que resumen la cantidad de brazas torcidas de orden $n \leq 868$ con algunas excepciones. Es importante destacar que ninguna de esas excepciones es de la forma p^2q con p y q números primos distintos. Toda esta información se encuentra disponible en [69] y fue de una inestimable ayuda a lo largo de este trabajo. Todos nuestros resultados coinciden con las tablas mencionadas.

Relaciones	Cantidad	Sección
$p = 1 \pmod q,\ q > 2$	$\frac{q+15}{2}$	§ 4.2
$p = 1 \pmod q,\ q = 2$	8	§ 4.2
$p = -1 \pmod q$	5	§ 4.3
$q = 1 \pmod p,\ q \neq 1 \pmod{p^2}$	$p + 8$	§ 4.4
$q = 1 \pmod{p^2}$	$2p + 8$	§ 4.5
$p = 2,\ q \neq 1 \pmod 4$	9	§ 4.6
$p = 2,\ q = 1 \pmod 4$	11	§ 4.7
p y q aritméticamente independientes	4	§ 4.8

Tabla 4.1: Enumeración de brazas de orden p^2q.

En [13, Conjecture 4.1], los autores conjeturan la cantidad de brazas torcidas de orden p^2q a partir de los resultados obtenidos en sus tablas. Como aplicación, en el teorema 5.5.1 daremos una respuesta positiva a dicha conjetura.

4.1. Preliminares

Lema 4.1.1. *Sean p, q dos números primos distintos con $p > 2$ y sea $(A, +, \circ)$ una braza torcida finita de orden p^2q.*

(i) Si $p = \pm 1 \pmod q$ entonces el único p-subgrupo de Sylow de $(A, +)$ es un ideal. En particular, los p-subgrupos de Sylow de $(A, +)$ y $(A, \circ)$ son isomorfos.

(ii) Si $q = 1 \pmod p$ entonces el único q-subgrupo de Sylow de $(A, +)$ es un ideal.

Demostración. Los grupos de orden p^2q con $p = \pm 1 \pmod q$ contienen un único p-subgrupo de Sylow por lo cual es un subgrupo característico. Por lo tanto, si denotamos por P al único p-subgrupo de Sylow de $(A, +)$ tenemos que para todo $x \in A$, $\lambda_x(P) = P$. Al tener orden p^2, P es el único p-subgrupo de Sylow de $(A, \circ)$ (ya que los ideales a izquierda son subgrupos de la estructura multiplicativa). Luego, es normal en $(A, \circ)$ y por lo tanto es un ideal. En particular $(P, +, \circ)$ es una braza torcida de orden p^2 y de acuerdo a la clasificación de [7] tenemos que $(P, +) \cong (P, \circ)$. El mismo argumento se utiliza para demostrar (ii). □

Para hallar las fórmulas que definen la operación multiplicativa de las brazas torcidas que clasificaremos, vamos a utilizar el siguiente lema con mucha frecuencia.

Lema 4.1.2. *Sea A una braza torcida.*

(i) Si $\lambda_b(b) = b$ entonces

$$\underbrace{b \circ b \circ \ldots \circ b}_{n} = nb \quad y \quad \lambda_{nb} = \lambda_b^n$$

para todo $n \in \mathbb{N}$ donde $nb = \underbrace{b + b + \ldots + b}_{n}$.

(ii) Si $a, c \in \ker \lambda$ y $b, d \in \mathrm{Fix}(A)$ entonces

$$(a + b) \circ (c + d) = a + b + \lambda_b(c) + d.$$

Demostración. (i) Se sigue por inducción en n, puesto que si $\lambda_b(b) = b$ entonces $b \circ b = b + \lambda_b(b) = b + b = 2b$ y $\lambda_{2b} = \lambda_{b \circ b} = \lambda_b^2$.

(ii) Sean $a, c \in \ker \lambda$ y $b, d \in \mathrm{Fix}(A)$. Entonces

$$(a + b) \circ (c + d) = a + b + \lambda_{a \circ b}(c + d) = a + b + \lambda_b(c + d) = a + b + \lambda_b(c) + d$$

donde estamos usando que $\lambda_{a+b} = \lambda_{a \circ b} = \lambda_b$ pues $a \in \ker \lambda$. □

4.1.1. Brazas torcidas y subgrupos regulares

Como mencionamos en la sección 3.2 del capítulo 3, retomaremos a continuación la construcción de subgrupos regulares que será la clave de todo lo que sigue. Algunas observaciones fueron hechas en el capítulo anterior pero preferimos recordarlas para facilitar la lectura.

Recordemos que la acción de un grupo de permutaciones G sobre un conjunto X se dice *regular* si, para cada par de elementos $x, y \in X$, existe un único elemento $g \in G$ tal que $g(x) = y$. El *holomorfo* $\mathrm{Hol}(A) = A \rtimes \mathrm{Aut}\, A$ de un grupo A se identifica con un subgrupo del grupo de permutaciones de A. En efecto, la acción de un elemento $(a, f) \in \mathrm{Hol}(A)$ sobre A está dada por

$$(a, f) \cdot x = a + f(x) \tag{4.1}$$

para todo $x \in A$ donde la operación del grupo A la escribimos en notación aditiva. En consecuencia, diremos que un subgrupo G de $\mathrm{Hol}(A)$ es *regular* si la imagen de G en el grupo de permutaciones de A mediante esta identificación es regular.

Podemos definir una acción de $\mathrm{Aut}(A, +)$ sobre $\mathrm{Hol}(A, +)$ dada por la conjugación donde identificamos $\mathrm{Aut}(A, +)$ con el subgrupo $1 \times \mathrm{Aut}\, A \leq \mathrm{Hol}(A, +)$.

En [41], se mostró que a partir de un grupo $(A, +)$ existe una correspondencia biunívoca entre clases de isomorfismo de brazas torcidas $(A, +, \circ)$ y las órbitas de los subgrupos regulares $\mathrm{Hol}(A, +)$ bajo la acción de conjugación por $\mathrm{Aut}(A, +)$ del párrafo anterior.

Consideraremos

$$\pi_1 : \mathrm{Hol}(A) \longrightarrow A \qquad\qquad \pi_2 : \mathrm{Hol}(A) \longrightarrow \mathrm{Aut}\, A$$
$$(a, f) \mapsto a \qquad\qquad (a, f) \mapsto f$$

las sobreyecciones canónicas.

4.1.2. Subgrupos regulares

En esta sección vamos a resumir la estrategia general que utilizamos para encontrar subgrupos regulares del holomorfo de un cierto grupo finito A. Además, fijamos notación y terminología que utilizaremos en lo que sigue. El método está inspirado en [52, Section 2.2]. Consideramos π_1 y π_2 como antes. La función π_1 nos ayuda a verificar la regularidad de un subgrupo $G \leq \mathrm{Hol}(A)$ con $|G| = |A|$.

Podemos identificar al elemento $(a, f) \in \mathrm{Hol}(A, +)$ con una permutación del conjunto A actuando como $(a, f) \cdot x = a + f(x)$ para todo $x \in A$.

Si $(a, f), (b, g) \in G$ entonces

$$\pi_1(a, f) = \pi_1(b, g) \text{ si y sólo si } (a, f)^{-1}(b, g) \in H = G \cap (\{1\} \times \mathrm{Aut}\, A).$$

Luego la función π_1 restingida a G se factoriza por la proyección canónica sobre el conjunto de coclases con respecto al subgrupo H. Si G es finito, tenemos que $|G| = |H||\pi_1(G)|$ y $|\pi_1(G)|$ divide al orden de G.

Lema 4.1.3. *Sea A un grupo finito y $G \leq \mathrm{Hol}(A)$. Son equivalentes:*

(i) G es regular;

(ii) $|A| = |G|$ y $\pi_1(G) = A$;

(iii) $|A| = |G|$ y $G \cap (1 \times \mathrm{Aut}\, A) = 1$.

Demostración. Sea θ la acción canónica definida por (4.1). Como esta acción es fiel y A es finito tenemos que son equivalentes:

(i) G es regular;

(ii) $|A| = |G|$ y la órbita de 1 por θ es A;

(iii) $|A| = |G|$ y el estabilizador de 1 bajo la acción de G es trivial.

El estabilizador de 1 bajo la acción θ es $G \cap (1 \times \mathrm{Aut}\, A)$ y la órbita de 1 es $\pi_1(G)$. De esto, se sigue el enunciado. □

Lema 4.1.4. *Sean A un grupo y $G = \langle u_i\alpha_i,\, i \in I\rangle \leq \mathrm{Hol}(A)$ donde $u_i \in A$, $\alpha_i \in \mathrm{Aut}\, A$ para $i \in I$. Entonces:*

(1) $\pi_1(G) \subseteq \langle h(g) \mid g \in U,\, h \in \pi_2(G)\rangle$, donde $U = \langle u_i,\, i \in I\rangle$.

(2) Si $\alpha_i(u_i) = u_i$ entonces $\langle u_i\rangle \subseteq \pi_1(G)$.

Demostración. (1) Tenemos que

$$u_i\alpha_i x f = u_i\alpha_i(x)\alpha_i f \quad \text{y} \quad (u_i\alpha_i)^{-1} = \alpha_i^{-1}(u_i)^{-1}\alpha_i^{-1}, \tag{4.2}$$

para cualesquiera $i \in I$, $x \in A$ y $f \in \operatorname{Aut} A$, de lo cual se deduce la afirmación por inducción.

(2) Por (4.2) tenemos que

$$(u_i\alpha_i)^n = u_i^n\alpha_i^n$$

y entonces $\pi_1((u_i\alpha_i)^n) = u_i^n$ para todo $n \in \mathbb{Z}$. □

Para mostrar que un subgrupo G del holomorfo de A es regular usaremos los lemas 4.1.3 y 4.1.4 o bien verificaremos directamente que el estabilizador de la identidad es trivial.

Como estrategia general, mostraremos una lista de representantes de subgrupos regulares y luego probaremos que todo subgrupo regular es conjugado de alguno de los grupos de la lista. A continuación detallamos los dos grandes pasos de la estrategia.

En primer lugar, buscamos una lista de subgrupos regulares del holomorfo que no sean conjugados entre sí teniendo en cuenta ciertas propiedades que son invariantes por la conjugación por elementos del subgrupo $1 \times \operatorname{Aut} A$ de $\operatorname{Hol}(A)$.

Sea G un subgrupo de $\operatorname{Hol}(A)$, entonces la clase de conjugación de $\pi_2(G)$ en $\operatorname{Aut} A$ y en particular $|\pi_2(G)|$ son invariantes. La función π_2 es un morfismo de grupos y el cardinal de la imagen por π_2 divide tanto a $|(A,+)|$ como a $|\operatorname{Aut}(A,+)|$, por lo tanto divide al máximo común divisor. Si la imagen por π_2 es trivial, hay una única *skew brace* asociada y es la trivial definida sobre A.

Si dos grupos G y H tienen la misma imagen por π_2 y son conjugados por un cierto h, entonces h normaliza su imagen por π_2 y $\ker \pi_2|_G = h(\ker \pi_2|_H)h^{-1}$. Luego el núcleo con respecto a π_2 se puede modificar actuando por el normalizador de la imagen de π_2. Por lo tanto, para el primer paso, necesitamos:

- Hallar el máximo común divisor entre $|A|$ y $|\operatorname{Aut} A|$.
- Para cada k que divide al máximo común divisor, encontrar las clases de conjugación de subgrupos de orden k de $\operatorname{Aut}(A,+)$. Si $\operatorname{Aut} A$ es abeliano, debemos calcular todos los subgrupos del orden dado.
- El núcleo de π_2 es un subgrupo de $\operatorname{Hol}(A)$ que está contenido en $A \times 1$. Luego, debemos hallar una familia de representantes de las órbitas de los subgrupos de orden $\frac{|A|}{k}$ de A, bajo la acción del normalizador de la imagen por π_2 en A.

En algunos casos, los invariantes generales de antes no alcanzan para identificar la clase de conjugación de subgrupos regulares en el sentido del teorema 3.1.3 y debemos introducir argumentos *ad hoc* que dependen de la estructura particular de A y sus automorfismos. Otros argumentos que nos resultarán de utilidad son los siguientes. Supongamos que G y H son subgrupos regulares de $\operatorname{Hol}(A)$ que son conjugados por un elemento $h \in \operatorname{Aut} A$, entonces:

- los p-subgrupos de Sylow de G son conjugados por h a los p-subgrupos de Sylow de H.
- sea $\mathfrak{H}$ un subgrupo normal de $\mathrm{Hol}(A)$. El siguiente diagrama conmuta:

$$\begin{array}{ccc} \mathrm{Hol}(A) & \xrightarrow{\widehat{h}} & \mathrm{Hol}(A) \\ \downarrow & & \downarrow \\ \mathrm{Hol}(A)/\mathfrak{H} & \xrightarrow{\widehat{h\mathfrak{H}}} & \mathrm{Hol}(A)/\mathfrak{H} \end{array} \tag{4.3}$$

  donde $\widehat{h}$, $\widehat{h\mathfrak{H}}$ son los automorfismos interiores y las flechas hacia abajo son los morfismos canónicos. Entonces sus imágenes en el cociente $\mathrm{Hol}(A)/\mathfrak{H}$ son conjugadas por $h\mathfrak{H}$. Luego, la clase de conjugación de la imagen en el cociente $\mathrm{Hol}(A)/\mathfrak{H}$ es invariante salvo conjugación.

Usando el lema 4.1.3 y diferentes invariantes podemos dar una lista de subgrupos regulares para cada valor de k posible que no sean conjugados entre sí.

Las clases de isomorfismos de los subgrupos listados como representantes de las clases de conjugación se pueden calcular fácilmente utilizando la lista de grupos de orden p^2q por lo cual omitimos la demostración de cada caso.

El segundo paso consiste en probar que todo subgrupo regular es conjugado a uno de la lista hallada en el primer paso. En particular, debemos describir a los subgrupos de $\mathrm{Hol}(A)$ de acuerdo a los invariantes mencionados anteriormente.

Denotaremos por $\{\alpha_i : 1 \leq i \leq n\}$ a un conjunto de generadores de $\pi_2(G)$ y por $\{k_j : 1 \leq j \leq m\}$ a un conjunto de generadores del núcleo de $\pi_2|_G$. Un subgrupo regular G se puede dar de la siguiente manera:

$$G = \langle k_1, \ldots, k_m, u_1\alpha_1, \ldots, u_n\alpha_n \rangle,$$

para ciertos $u_i \in A$. De acuerdo al lema 4.1.3, $u_i \neq 1$ puesto que G es regular. Nos referiremos a esta presentación del grupo G como la *presentación estándar* de G. Cabe destacar que podemos modificar al elemento u_i por cualquier otro de su misma coclase con respecto al núcleo sin que esto modifique al grupo G (dado que esto se traduce en la multiplicación por la izquierda de los elementos $u_i\alpha_i$ por elementos del núcleo). Más aún, así como ocurre en cualquier grupo, todo generador puede ser multiplicado por cualquier elemento de G sin que ello modifique al propio grupo. Utilizaremos estas operaciones cuando nos ayuden a simplificar los cálculos sin mayor justificación.

El grupo regular G debe satisfacer las siguientes condiciones que nos darán restricciones a la hora de elegir los elementos u_i:

(K) El núcleo de $\pi_2|_G$ es normal en G.

(R) Los generadores $\{u_i\alpha_i : 1 \leq i \leq n\}$ satisfacen las mismas relaciones que $\{\alpha_i : 1 \leq i \leq n\}$ modulo $\ker \pi_2|_G$ (por ejemplo, si $\alpha_i^n = 1$ entonces tenemos que $(u_i\alpha_i)^n \in \ker \pi_2|_G$).

Dado un grupo regular, podemos conjugarlo por elementos del normalizador de $\pi_2(G)$ en Aut A que estabilizan al núcleo de $\pi_2|_G$ para ver que G es conjugado a uno de los representantes elegidos.

4.1.3. Notación

En lo que sigue, vamos a fijar p y q como dos números primos diferentes. Denotaremos, como es usual, mediante $\mathbb{Z}_n^\times$ al grupo de unidades de $\mathbb{Z}_n$ con la operación de multiplicación. Para los dos grupos abelianos de orden p^2q utilizaremos las presentaciones:

(i) $\mathbb{Z}_{p^2q} = \langle \sigma, \tau \mid \sigma^{p^2} = \tau^q = 1,\ [\sigma, \tau] = 1 \rangle$;

(ii) $\mathbb{Z}_p^2 \times \mathbb{Z}_q = \langle \sigma, \tau, \epsilon \mid \sigma^p = \tau^p = \epsilon^q = 1,\ [\sigma, \tau] = [\sigma, \epsilon] = [\tau, \epsilon] = 1 \rangle$.

El grupo de automorfismos de $\mathbb{Z}_{p^2q}$ es isomorfo a $\mathbb{Z}_{p^2}^\times \times \mathbb{Z}_q^\times$ por lo cual su orden es $p(p-1)(q-1)$. Denotamos por $\varphi_{i,j}$ el automorfismo dado por

$$\sigma \mapsto \sigma^i \qquad \text{y} \qquad \tau \mapsto \tau^j$$

donde $i \in \mathbb{Z}_{p^2}^\times$ y $j \in \mathbb{Z}_q^\times$.

El grupo de automorfismos de $\mathbb{Z}_p^2 \times \mathbb{Z}_q$ es isomorfo a $GL_2(p) \times \mathbb{Z}_q^\times$ cuyo orden es $p(p-1)^2(p+1)(q-1)$. Podemos representar a los automorfismos de $\mathbb{Z}_p^2 \times \mathbb{Z}_q$ como $M\alpha$ donde M es una matriz inversible en la base σ, τ y $\alpha \in \mathbb{Z}_q^\times$.

Notemos que en ambos casos los subgrupos de Sylow son característicos y, por lo tanto, normales en el holomorfo.

Si C es un grupo cíclico actuando sobre un grupo G mediante $\rho : C \longrightarrow \text{Aut}\, G$ y $\rho(1) = f$ entonces $G \rtimes_f C$ denota el producto semidirecto determinado por la acción ρ (que queda determinado por la imagen del generador de C por ρ).

4.2. Brazas de orden p^2q con $p = 1 \pmod q$

A lo largo de esta sección asumiremos que p y q son números primos tales que $p = 1 \pmod q$, incluyendo el caso $q = 2$ salvo indicación contraria.

En [27, §5.1 y §5.3] Crespo clasifica las brazas de orden $2p^2$. Recuperaremos sus resultados como un caso particular. Denotaremos por $\mathfrak{B}$ al subconjunto de $\mathbb{Z}_q$ formado por $0, 1, -1$ y un valor entre k y k^{-1} si $k \neq 0, 1, -1$. Para $q = 2$ tomaremos $\mathfrak{B} = \{0, 1\}$. Notar que si $q > 2$ entonces $|\mathfrak{B}| = \frac{q+3}{2}$. Fijaremos un elemento g de orden q en $\mathbb{Z}_p^\times$ y un elemento t de orden q in $\mathbb{Z}_{p^2}^\times$.

De acuerdo con [14, Proposition 21.17], los grupos no abelianos de orden p^2q son los siguientes:

(i) $\mathbb{Z}_{p^2} \rtimes_t \mathbb{Z}_q \cong \langle \sigma, \tau \mid \sigma^{p^2} = \tau^q = 1,\ \tau\sigma\tau^{-1} = \sigma^t \rangle$;

(ii) $\mathcal{G}_k = \langle \sigma, \tau, \epsilon \,|\, \sigma^p = \tau^p = \epsilon^q = 1,\ \epsilon\sigma\epsilon^{-1} = \sigma^g,\ \epsilon\tau\epsilon^{-1} = \tau^{g^k} \rangle \cong \mathbb{Z}_p^2 \rtimes_{\mathcal{D}_{1,k}} \mathbb{Z}_q$, donde $\mathcal{D}_{1,k}$ es la matriz diagonal con entradas g, g^k para $k \in \mathfrak{B}$.

Notemos que si $q = 2$, el grupo (i) es isomorfo al grupo diedral de orden $2p^2$ y podemos asumir que $t = -1$. Los grupos del ítem (ii) se pueden parametrizar utilizando al conjunto $\mathfrak{B}$ puesto que $\mathcal{G}_k$ y $\mathcal{G}_{k^{-1}}$ son isomorfos si $k \neq 0, 1, -1$. En particular, tenemos $\frac{q+3}{2}$ clases de isomorfismos de grupos de orden p^2q si $q > 2$ y sólo 2 clases si $q = 2$.

En la siguiente tabla recopilamos la enumeración de las brazas de esta sección de acuerdos a la clase de isomorfismo de sus grupos aditivos y multiplicativos.

$+\backslash\circ$	$\mathbb{Z}_{p^2q}$	$\mathbb{Z}_{p^2} \rtimes_t \mathbb{Z}_q$	$\mathbb{Z}_p^2 \times \mathbb{Z}_q$	$\mathcal{G}_k$, $k \in \mathfrak{B} \setminus \{2\}$	$\mathcal{G}_2$
$\mathbb{Z}_{p^2q}$	2	1	-	-	-
$\mathbb{Z}_p^2 \times \mathbb{Z}_q$	-	-	2	1	2

Tabla 4.2: Enumeración de brazas de orden p^2q con $p = 1 \pmod q$.

Merece una mención especial el caso $q = 3$ ya que en ese caso $\mathfrak{B} = \{0, 1, -1\}$, $2 = -1$ y por lo tanto tenemos 2 brazas de tipo $\mathbb{Z}_p^2 \times \mathbb{Z}_q$ con grupo multiplicativo isomorfo a $\mathcal{G}_{-1}$. Por otro lado, para el caso $q = 2$ tenemos que $2 = 0$ y entonces $\mathfrak{B} \setminus \{2\} = \{1\}$.

4.2.1. Brazas de tipo cíclico

En esta sección vamos a denotar por A al grupo cíclico $\mathbb{Z}_{p^2q}$ y utilizaremos la notación de la sección 4.1.3 para los generadores del grupo y sus automorfismos. Si G es un subgrupo regular de $\mathrm{Hol}(A)$ entonces $|\pi_2(G)|$ pertenece a $\{1, q, p, pq\}$ puesto que divide a $|\operatorname{Aut} A| = p(p-1)(q-1)$ y a p^2q. Veamos primero que no hay subgrupos regulares que cumplan la condición $|\pi_2(G)| = pq$.

Proposición 4.2.1. *Sea G un subgrupo regular de* $\mathrm{Hol}(A)$. *Entonces $|\pi_2(G)| \neq pq$.*

Demostración. El único subgrupo de $\operatorname{Aut} A$ de orden pq está generado por el automorfismo $\alpha = \varphi_{g(p+1),1}$ y el único subgrupo del orden p de A es $\langle \sigma^p \rangle$. Supongamos que G es un subgrupo de orden p^2q de $\mathrm{Hol}(A)$ con $\pi_2(G) = \langle \alpha \rangle$. Entonces, la presentación estándar de G es

$$G = \langle \sigma^p,\ \sigma^a \tau^b \alpha \rangle$$

para ciertos a, b. Dado que $(p+1)^m = pm + 1 \pmod{p^2}$ tenemos

$$(\sigma^a \tau^b \alpha)^q = \sigma^{a \frac{g^q (p+1)^q - 1}{g(p+1) - 1}} \tau^{bq} \alpha^q = \sigma^{a \frac{qp}{g(p+1)-1}} \alpha^q \in G.$$

Ahora, como $\sigma^p \in G$ entonces $\alpha^q \in G \cap (1 \times \operatorname{Aut} A)$ y, por el lema 4.1.3, G no es regular. □

Los siguientes teoremas valen bajo la condición más general de que $q \neq 1 \pmod p$ y serán aplicados más adelante por lo cual los enunciamos con toda generalidad.

Teorema 4.2.2. *Sean p, q números primos con $q \neq 1 \pmod p$. La única braza de tipo cíclico con $|\ker \lambda| = pq$ es $(B, +, \circ)$ donde*

$$\binom{n}{m} + \binom{s}{r} = \binom{n+s}{m+r}, \qquad \binom{n}{m} \circ \binom{s}{r} = \binom{n+s+pns}{m+r} \tag{4.4}$$

para todos $0 \leq n, s \leq p^2 - 1$ y $0 \leq m, r \leq q - 1$. En particular, $(B, \circ) \cong \mathbb{Z}_{p^2q}$.

Demostración. El único subgrupo de orden p de $\operatorname{Aut} A$ es el subgrupo generado por $\varphi_{p+1,1}$ y A tiene un único subgrupo de orden pq, digamos $\langle \sigma^p, \tau \rangle$. Suponiendo que G es un subgrupo regular de $\operatorname{Hol}(A)$ con $|\pi_2(G)| = p$ tenemos la siguiente presentación estándar:

$$G = \langle \sigma^p,\ \tau,\ \sigma^a \tau^b \varphi_{p+1,1} \rangle = \langle \sigma^p,\ \tau,\ \sigma^a \varphi_{p+1,1} \rangle,$$

donde $1 \leq a \leq p - 1$ y en particular G es abeliano. Por [22, Corollary 4.3], como las estructuras aditiva y multiplicativa de la braza asociada a G son abelianas entonces la braza se puede pensar como un producto directo de una braza de orden p^2 y la braza trivial de orden q. De acuerdo a la clasificación de brazas de orden p^2 dada en [7, Proposition 2.4], hay únicamente una braza no trivial de orden p^2 con grupo aditivo cíclico y eso nos lleva a la fórmula (4.4). El grupo $(B, \circ)$ es cíclico pues de acuerdo con el lema 4.1.1, su p-subgrupo de Sylow es cíclico. □

Teorema 4.2.3. *Sean p, q números primos tales que $q \neq 1 \pmod p$. La única braza de tipo cíclico con $|\ker \lambda| = p^2$ es $(B, +, \circ)$ donde*

$$\binom{n}{m} + \binom{s}{r} = \binom{n+s}{m+r}, \qquad \binom{n}{m} \circ \binom{s}{r} = \binom{n+t^m s}{m+r}. \tag{4.5}$$

para todos $0 \leq n, s \leq p^2 - 1$ y $0 \leq m, r \leq q - 1$. En particular, $(B, \circ) \cong \mathbb{Z}_{p^2} \rtimes_t \mathbb{Z}_q$ y $(B, +, \circ)$ es una bi-braza.

Demostración. Por el corolario 3.1.2, tenemos que (4.5) define una bi-braza con las propiedades deseadas. Veamos que existe una única braza con las condiciones del enunciado. El único subgrupo de orden q de $\operatorname{Aut} A$ es el subgrupo generado por $\varphi_{t,1}$. El único subgrupo de orden p^2 de A está generado por σ. Sea G un subgrupo regular con $|\pi_2(G)| = q$, entonces G tiene la siguiente presentación estándar:

$$G_b = \langle \sigma,\ \tau^b \varphi_{t,1} \rangle,$$

con $1 \leq b \leq q - 1$. El grupo G_b es conjugado del subgrupo

$$H = \langle \sigma, \tau \varphi_{t,1} \rangle \cong \mathbb{Z}_{p^2} \rtimes_t \mathbb{Z}_q$$

por $\varphi_{1,b}^{-1}$. Por lo tanto existe una única braza bajo las condiciones del enunciado salvo isomorfismo. □

Resumimos a continuación los resultados parciales obtenidos en esta subsección. Las columnas hacen referencia a la clase de isomorfismo del grupo multiplicativo.

$\lvert\ker\lambda\rvert$	$\mathbb{Z}_{p^2q}$	$\mathbb{Z}_{p^2} \rtimes_t \mathbb{Z}_q$
pq	1	-
p^2	-	1
p^2q	1	-

Tabla 4.3: Enumeración de las brazas de tipo cíclico de orden p^2q con $p = 1 \pmod q$.

4.2.2. Brazas de tipo $\mathbb{Z}_p^2 \times \mathbb{Z}_q$

Notemos ahora por A al grupo abeliano $\mathbb{Z}_p^2 \times \mathbb{Z}_q$. Si G es un subgrupo regular de $\mathrm{Hol}(A)$ entonces $|\pi_2(G)|$ divide tanto a p^2q como a $|\operatorname{Aut} A| = p(p-1)^2(p+1)(q-1)$. Por lo tanto $|\pi_2(G)|$ es un divisor de pq pues $p = 1 \pmod q$.

Observación 4.2.4. Los automorfismos de A de orden p, q o pq actúan trivialmente sobre sus q-subgrupos de Sylow puesto que p y q no dividen a $q-1$. Por lo tanto, si G es un subgrupo regular de orden p^2q entonces la acción de $\pi_2(G)$ sobre el q-subgrupo de Sylow de A es trivial.

Observación 4.2.5. Supongamos que p y q son números primos tales que $p = 1 \pmod q$ y g es un elemento de orden q en $\mathbb{Z}_p^\times$. Si denotamos por $\mathcal{D}_{a,b}$ a la matriz diagonal que en la diagonal tiene a los elementos g^a y g^b, vamos a considerar las matrices

$$C = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad \mathcal{D}_{1,s} = \begin{bmatrix} g & 0 \\ 0 & g^s \end{bmatrix} \quad \text{y} \quad \mathcal{D}_{0,1} = \begin{bmatrix} 1 & 0 \\ 0 & g \end{bmatrix}$$

para $0 \le s \le q-1$. Es un hecho conocido que, salvo conjugación, los subgrupos de orden q de $GL_2(p)$ están generados por una de las matrices $\mathcal{D}_{1,s}$ con $s \in \mathfrak{B}$ (incluyendo el caso $q = 2$). Notemos además que $\mathcal{D}_{0,1}$ es conjugada de $\mathcal{D}_{1,0}$.

Los subgrupos de orden p de $GL_2(p)$ son sus p-subgrupos de Sylow y entonces son todos conjugados del subgrupo generado por C.

Un conjunto de representantes de las clases de conjugación de los subgrupos de orden pq de $GL_2(p)$ viene dado por $H_s = \langle C, \mathcal{D}_{1,s}\rangle$ y $\widetilde{H} = \langle C, \mathcal{D}_{0,1}\rangle$, donde $0 \le s \le q-1$. De hecho, salvo conjugación, podemos asumir que el p-subgrupo de Sylow de un grupo H de orden pq está generado por C. Luego, el generador de orden q es una matriz triangular superior pues pertenece al normalizador de C por lo cual podemos suponer que H está generado por C y por una matriz diagonal de orden q que puede ser o bien alguna de las $\mathcal{D}_{1,s}$ para $0 \le s \le q-1$ o bien $\mathcal{D}_{0,1}$. Estas matrices no son conjugadas por elementos del normalizador de C y por lo tanto los subgrupos correspondientes no son conjugados.

En el siguiente teorema asumimos nuevamente que $q \neq 1 \pmod p$ al igual que hicimos en el teorema 4.2.2.

Teorema 4.2.6. *Sean p, q números primos tales que $q \neq 1 \pmod p$. La única braza de tipo A con $|\ker\lambda| = pq$ es $(B, +, \circ)$ donde*

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \\ x_3 + y_3 \end{pmatrix}, \qquad \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \circ \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} x_1 + y_1 + x_2y_2 \\ x_2 + y_2 \\ x_3 + y_3 \end{pmatrix} \tag{4.6}$$

para todos $0 \leq x_1, x_2, y_1, y_2 \leq p-1$, $0 \leq x_3, y_3 \leq q-1$.

En particular, $(B, \circ) \cong \mathbb{Z}_p^2 \times \mathbb{Z}_q$.

Demostración. Sea $G \leq \mathrm{Hol}(A)$ un subgrupo regular con $|\pi_2(G)| = p$. De acuerdo con las observaciones 4.2.4 y 4.2.5 y el hecho de que $q \neq 1 \pmod p$ podemos asumir que $\pi_2(G)$ está generado por C, salvo conjugación. Luego, el grupo G tiene la siguiente presentación estándar:

$$G = \langle v,\ \epsilon,\ \sigma^a \tau^b C \rangle$$

para ciertos $0 \leq a, b \leq p-1$ y $v \in \langle \sigma, \tau \rangle$. La condición (K) que definimos en la página 48 implica que $v \in \langle \sigma \rangle$ y entonces G es abeliano. Por lo tanto, tanto la estructura aditiva como la multiplicativa de la braza que se obtiene de G son abelianas y entonces por [22, Corollary 4.3] se pueden escribir como un producto directo de una braza de orden p^2 y una braza trivial de orden q. De acuerdo con la clasificación de brazas de orden p^2 dada en [7, Proposition 2.4], existe una única braza no trivial y tenemos entonces la fórmula (4.6). Por el lema 4.1.1, el grupo $(B, \circ)$ es isomorfo a A pues su p-subgrupo de Sylow es elemental abeliano. □

Teorema 4.2.7. *Sean* p, q *números primos tales que* $p = 1 \pmod q$. *Las brazas de tipo* A *con* $|\ker \lambda| = p^2$ *son de la forma* $B_s = (A, +, \circ)$ *para* $s \in \mathfrak{B}$ *donde*

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \\ x_3 + y_3 \end{pmatrix}, \qquad \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \circ \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} x_1 + g^{x_3} y_1 \\ x_2 + (g^s)^{x_3} y_2 \\ x_3 + y_3 \end{pmatrix} \tag{4.7}$$

para todos $0 \leq x_1, x_2, y_1, y_2 \leq p-1$, $0 \leq x_3, y_3 \leq q-1$. *En particular* $(B_s, \circ) \cong \mathcal{G}_s$ *y* B_s *es una bi-braza.*

Demostración. Los grupos

$$H_s = \langle \sigma,\ \tau,\ \epsilon \mathcal{D}_{1,s} \rangle \cong \mathcal{G}_s, \tag{4.8}$$

para $s \in \mathfrak{B}$ no son conjugados dos a dos pues sus imágenes por π_2 no lo son y $|\pi_2(H_s)| = q$.

Sean $K = \langle \sigma, \tau \rangle$ y $p : \mathrm{Hol}(A) \longrightarrow \mathrm{Hol}(A)/K \cong \mathbb{Z}_q \times \mathrm{Aut}\, A$. Asumamos que $h \in (1 \times \mathrm{Aut}\, A) \cap H_s$. Entonces $p(h) \in (1 \times \mathrm{Aut}\, A) \cap \langle \epsilon \mathcal{D}_{1,s} \rangle = 1$. En consecuencia, $h \in K \cap (1 \times \mathrm{Aut}\, A) = 1$. Por lo tanto, por el lema 4.1.3 H_s es regular.

Veamos ahora que todo subgrupo regular G con $|\pi_2(G)| = q$ es un conjugado de alguno de los subgrupos de (4.8). El núcleo de $\pi_2|_G$ es el p-subgrupo de Sylow de A y la imagen de $\pi_2|_G$ está generada por un automorfismo de orden q. Luego, de acuerdo con las observaciones 4.2.4 y 4.2.5 podemos suponer que el automorfismo está dado por $\mathcal{D}_{1,s}$ para algún $s \in \mathfrak{B}$. Por lo tanto

$$G = \langle \sigma,\ \tau,\ \epsilon^a \mathcal{D}_{1,s} \rangle$$

para cierto $a \neq 0$ pues G es regular. Entonces G es el conjugado de H_s por el automorfismo de $\mathbb{Z}_q$ que transforma ϵ en $\epsilon^{a^{-1}}$.

Sea B_s la braza asociada a H_s. Entonces $\sigma, \tau \in \ker\lambda$ y $\epsilon \in \mathrm{Fix}(B_s)$, por lo que podemos aplicar el lema 4.1.2(ii), es decir

$$\begin{aligned}\sigma^n\tau^m\epsilon^l \circ \sigma^x\tau^y\epsilon^z &= \sigma^n\tau^m\epsilon^l\lambda_{\sigma^n\tau^m\epsilon^l}(\sigma^x\tau^y\epsilon^z)\\ &= \sigma^n\tau^m\epsilon^l\lambda_\epsilon^l(\sigma^x\tau^y\epsilon^z)\\ &= \sigma^n\tau^m\lambda_\epsilon^l(\sigma^x\tau^y)\epsilon^{l+z} = \sigma^n\tau^m\mathcal{D}_{1,s}^l(\sigma^x\tau^y)\epsilon^{l+z}\end{aligned}$$

para todos $0 \le n, m, x, y \le p-1$, $0 \le l, z \le q-1$. Entonces se sigue la fórmula (4.7) y las brazas B_s son bi-brazas por [1, Proposition 1.1], pues $(A,+) = \mathbb{Z}_p^2 \times \mathbb{Z}_q$ y $(A,\circ) = \mathbb{Z}_p^2 \rtimes_{\mathcal{D}_s} \mathbb{Z}_q$. □

Proposición 4.2.8. *Sea $q > 2$. La única braza de tipo A con $|\ker\lambda| = p$ es $(B,+,\circ)$ donde*

$$\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix} + \begin{pmatrix}y_1\\y_2\\y_3\end{pmatrix} = \begin{pmatrix}x_1+y_1\\x_2+y_2\\x_3+y_3\end{pmatrix}, \quad \begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix} \circ \begin{pmatrix}y_1\\y_2\\y_3\end{pmatrix} = \begin{pmatrix}x_1 + g^{x_3}y_1 + g^{2^{-1}x_3}x_2y_2\\ x_2 + g^{2^{-1}x_3}y_2\\ x_3+y_3\end{pmatrix} \tag{4.9}$$

para todos $0 \le x_1, x_2, y_1, y_2 \le p-1$, $0 \le x_3, y_3 \le q-1$. En particular, $(B,\circ) \cong \mathcal{G}_2$.

Demostración. La imagen por π_2 del grupo

$$H = \langle \sigma,\ \tau C,\ \epsilon\mathcal{D}_{1,2^{-1}}\rangle \cong \mathcal{G}_{2^{-1}} \cong \mathcal{G}_2$$

tiene orden pq. Supongamos que $h = \sigma^n(\tau C)^m(\epsilon\mathcal{D}_{1,2^{-1}})^l = \sigma^{n+\frac{m(m-1)}{2}}\tau^m C^m\epsilon^l\mathcal{D}_{1,2^{-1}}^l$ pertenece al estabilizador de 1, es decir $\sigma^{n+\frac{m(m-1)}{2}}\tau^m\epsilon^l = 1$. Luego $n = m = l = 1$, por lo cual $h = 1$ y entonces H es regular pues $|H| = p^2q$.

Sea G un subgrupo regular de $\mathrm{Hol}(A)$ con $|\pi_2(G)| = pq$. Por las observaciones 4.2.4 y 4.2.5 podemos suponer que $\pi_2(G) = \langle C, \mathcal{D}_{1,s}\rangle$ para cierto valor de s o bien $\pi_2(G) = \langle C, \mathcal{D}_{0,1}\rangle$. En el primer caso, el grupo G tiene la siguiente presentación estándar

$$G = \langle v,\ u\epsilon^a C,\ w\epsilon^b\mathcal{D}_{1,s}\rangle,$$

donde $v, u, w \in \langle\sigma,\tau\rangle$. Verificando la condición (R) (véase p.48) para la condición $(u\epsilon^a C)^p \in \ker\pi_2|_G$ conseguimos $a = 0$ y por la condición (K) (véase p.48) tenemos que $v \in \langle\sigma\rangle$. Por lo tanto

$$G = \langle \sigma,\ \tau^a C,\ \tau^d\epsilon^b\mathcal{D}_{1,s}\rangle,$$

donde $a \neq 0$ pues G es regular. Conjugando por el automorfismo $a^{-1}I$ de $\mathbb{Z}_p^2$ podemos suponer que $a = 1$. Luego

$$G = \langle \sigma, \tau C, \tau^d\epsilon^b\mathcal{D}_{1,s}\rangle = \langle \sigma,\ \tau C,\ \epsilon^b C^{-d}\mathcal{D}_{1,s}\rangle$$

y por lo tanto $b \neq 0$. Conjugando ahora por el automorfismo b^{-1} de $\mathbb{Z}_q$ podemos suponer también que $b = 1$. Como

$$\begin{aligned}(\epsilon C^{-d}\mathcal{D}_{1,s})\tau C(\epsilon C^{-d}\mathcal{D}_{1,s})^{-1} &= \epsilon C^{-d}\mathcal{D}_{1,s}(\tau)\mathcal{D}_{1,s}C\mathcal{D}_{1,s}^{-1}C^d\epsilon^{-1}\\ &= \tau^{g^s}C^{g^{1-s}} \quad (\text{mód } \langle\sigma\rangle)\end{aligned} \tag{4.10}$$

y $C^{-d}\mathcal{D}_{1,s}C\mathcal{D}_{1,s}^{-1}C^d = C^{g^{1-s}}$, por la condición (R) tenemos

$$\tau^{g^s}C^{g^{1-s}} = (\tau C)^{g^{1-s}} = \tau^{g^{1-s}}C^{g^{1-s}} \pmod{\langle\sigma\rangle}$$

y entonces $1 - s = s \pmod q$, es decir $s = 2^{-1}$. Luego G es conjugado de H por C^n donde $n = \frac{d}{1-g^{2^{-1}}}$.

Sea B la braza asociada al subgrupo H. Entonces $\epsilon \in \mathrm{Fix}(B)$ y $\sigma \in \ker\lambda$, y entonces

$$\underbrace{\epsilon \circ \epsilon \circ \ldots \circ \epsilon}_{x_3} = \epsilon^{x_3}, \qquad \underbrace{\tau \circ \tau \circ \ldots \circ \tau}_{x_2} = \sigma^{\frac{x_2(x_2-1)}{2}}\tau^{x_2} = \sigma^{\frac{x_2(x_2-1)}{2}} \circ \tau^{x_2}$$

En consecuencia $\lambda_{\sigma^{x_1}\tau^{x_2}\epsilon^{x_3}} = \lambda_{\sigma^{x_1}\circ\tau^{x_2}\circ\epsilon^{x_3}} = \lambda_{\tau^{x_2}}\lambda_{\epsilon^{x_3}} = C^{x_2}\mathcal{D}_{1,2^{-1}}^{x_3}$. De esto se sigue la fórmula (4.9). Si $\pi_2(G) = \widetilde{H}$ podemos argumentar en forma análoga verificando las condiciones (R) y (K). De (4.10), reemplazando $\mathcal{D}_{1,s}$ por $\mathcal{D}_{0,1}$, obtenemos que $g^2 = 1$, una contradicción. □

Para la siguiente proposición, recordemos que g es un elemento fijo de orden q en $\mathbb{Z}_p^\times$, por lo cual para el caso $q = 2$ podemos asumir $g = -1$.

Proposición 4.2.9. *Sea $q = 2$. La única braza de tipo $\mathbb{Z}_p^2 \times \mathbb{Z}_2$ con $|\ker\lambda| = p$ es $(B, +, \circ)$ donde*

$$\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix} + \begin{pmatrix}y_1\\y_2\\y_3\end{pmatrix} = \begin{pmatrix}x_1+y_1\\x_2+y_2\\x_3+y_3\end{pmatrix}, \quad \begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix} \circ \begin{pmatrix}y_1\\y_2\\y_3\end{pmatrix} = \begin{pmatrix}x_1+y_1+(-1)^{x_3}x_2y_2\\x_2+(-1)^{x_3}y_2\\x_3+y_3\end{pmatrix} \quad (4.11)$$

para todos $0 \le x_1, x_2, y_1, y_2 \le p-1$, $0 \le x_3, y_3 \le 1$. En particular, $(B, \circ) \cong \mathcal{G}_0$.

Demostración. Podemos razonar de la misma forma que lo hicimos en la proposición 4.2.8. Sea G un subgrupo regular de $\mathrm{Hol}(A)$ con $\pi_2(G) = \langle C, \mathcal{D}_{1,s}\rangle$. Luego, como en la proposición 4.2.8 tenemos

$$G = \langle\sigma,\ \tau C,\ \tau^d\epsilon\mathcal{D}_{1,s}\rangle = \langle\sigma,\ \tau C,\ \epsilon C^{-d}\mathcal{D}_{1,s}\rangle$$

y entonces

$$(\epsilon C^{-d}\mathcal{D}_{1,s})\tau C(\epsilon C^{-d}\mathcal{D}_{1,s})^{-1} = \epsilon C^{-d}\mathcal{D}_{1,s}(\tau)\mathcal{D}_{1,s}C\mathcal{D}_{1,s}^{-1}C^d\epsilon^{-1} = \tau^{(-1)^s}C^{(-1)^{1-s}} \pmod{\langle\sigma\rangle}.$$

Por la condición (R), tenemos que

$$\tau^{(-1)^s}C^{(-1)^{1-s}} = (\tau C)^{(-1)^{1-s}} = \tau^{(-1)^{1-s}}C^{(-1)^{1-s}} \pmod{\langle\sigma\rangle}.$$

Entonces $(-1)^{1-s} = (-1)^s$ y se sigue que $-1 = 1$, por lo cual $p = 2$, una contradicción. En consecuencia, $\pi_2(G) = \widetilde{H}$ necesariamente. Usando las condiciones (R) y (K) tenemos que G es conjugado del siguiente grupo

$$K = \langle\sigma,\ \tau C,\ \epsilon\mathcal{D}_{0,1}\rangle.$$

Con la misma idea de la proposición 4.2.8 podemos ver que la braza asociada a G está dada por (4.11). □

Resumimos en la siguiente tabla los resultados obtenidos en esta subsección.

$\lvert\ker\lambda\rvert$	$\mathbb{Z}_p^2 \times \mathbb{Z}_q$	$\mathcal{G}_2$	$\mathcal{G}_k,\ k \in \mathfrak{B} \setminus \{2\}$
p	-	1	-
pq	1	-	-
p^2	-	1	1
p^2q	1	-	-

Tabla 4.4: Enumeración de las brazas de tipo $\mathbb{Z}_p^2 \times \mathbb{Z}_q$ con $p = 1 \pmod q$.
Para el caso $q = 2$, $\mathcal{G}_2 = \mathcal{G}_0$ y la última columna se corresponde con $\mathcal{G}_1$.
Notar que en el caso $q = 3$ tenemos que $2 = -1 \pmod 3$.

4.3. Brazas de orden p^2q con $p = -1 \pmod q$

En esta sección supondremos que p y q son números primos impares tales que $p = -1 \pmod q$ y que además $H = x^2 + \xi x + 1$ es un polinomio irreducible sobre $\mathbb{Z}_p$ tal que su matriz compañera

$$F = \begin{bmatrix} 0 & -1 \\ 1 & -\xi \end{bmatrix}$$

tiene orden q. Por [14, Proposition 21.17] existe un único grupo no abeliano de orden p^2q. Una presentación de este grupo aparece en [17]:

$$\mathcal{G}_F = \langle \sigma, \tau, \epsilon \,|\, \sigma^p = \tau^p = \epsilon^q = 1,\ \epsilon\sigma\epsilon^{-1} = \tau,\ \epsilon\tau\epsilon^{-1} = \sigma^{-1}\tau^{-\xi} \rangle \cong \mathbb{Z}_p^2 \rtimes_F \mathbb{Z}_q.$$

En la siguiente tabla resumimos la enumeración de brazas de orden p^2q según la clase de isomorfismo de sus grupos aditivos y multiplicativos con $p = -1 \pmod q$:

$+\backslash\circ$	$\mathbb{Z}_{p^2q}$	$\mathbb{Z}_p^2 \times \mathbb{Z}_q$	$\mathcal{G}_F$
$\mathbb{Z}_{p^2q}$	2	-	-
$\mathbb{Z}_p^2 \times \mathbb{Z}_q$	-	2	1

Tabla 4.5: Enumeración de brazas de orden p^2q con $p = -1 \pmod q$.

4.3.1. Brazas de tipo cíclico

A continuación, consideremos al grupo cíclico $\mathbb{Z}_{p^2q}$. En este caso, el orden de $\pi_2(G)$ para un subgrupo regular G de $\mathrm{Hol}(\mathbb{Z}_{p^2q})$ divide a p. Como en este caso $q \neq 1 \pmod p$ podemos aplicar el teorema 4.2.2 y por lo tanto la siguiente tabla resume la enumeración de las brazas de tipo cíclico.

$\lvert\ker\lambda\rvert$	$\mathbb{Z}_{p^2q}$
pq	1
p^2q	1

Tabla 4.6: Cantidad de brazas de tipo $\mathbb{Z}_{p^2q}$ de orden p^2q con $p = -1 \pmod q$.

4.3.2. Brazas de tipo $\mathbb{Z}_p^2 \times \mathbb{Z}_q$

Sean $A = \mathbb{Z}_p^2 \times \mathbb{Z}_q$ y G un subgrupo regular de $\mathrm{Hol}(A)$. Luego, el orden de $\pi_2(G)$ divide a p^2q y a $|\operatorname{Aut} A|$. Es decir, divide a pq pues $p = -1 \pmod q$.

Proposición 4.3.1. *Sea G un subgrupo regular de $\mathrm{Hol}(A)$. Entonces $|\pi_2(G)| \neq pq$.*

Demostración. Sea G un tal grupo, entonces $\ker \pi_2$ es un subgrupo normal de orden p de G. Por lo tanto G no es isomorfo a $\mathcal{G}_F$ pues este grupo no tiene subgrupos normales de orden p. Por otro lado, G no es abeliano pues $\operatorname{Aut} A$ no tiene subgrupos abelianos de orden pq. □

Lema 4.3.2. *Existe una única braza de tipo A con $|\ker \lambda| = p^2$ que está dada por $(B, +, \circ)$ donde*

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \\ x_3 + y_3 \end{pmatrix}, \qquad \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \circ \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + F^{x_3} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \\ x_3 + y_3 \end{pmatrix} \tag{4.12}$$

para todos $0 \leq x_1, x_2, y_1, y_2 \leq p-1$, $0 \leq x_3, y_3 \leq q-1$. En particular, $(B, \circ) \cong \mathcal{G}_F$ y B es una bi-braza.

Demostración. Sea G un subgrupo regular de $\mathrm{Hol}(A)$ con $|\pi_2(G)| = q$. Cualquier automorfismo de orden q de A actúa trivialmente sobre los q-subgrupos de Sylow de A. Salvo conjugación, podemos suponer que $\pi_2(G)$ está generado por F. Por lo tanto,

$$G = \langle \sigma,\ \tau,\ \sigma^n \tau^m \epsilon^a F \rangle = \langle \sigma,\ \tau,\ \epsilon^a F \rangle$$

donde $a \neq 0$ pues G es regular. Conjugando G por el automorfismo que transforma ϵ^a en ϵ y que fija σ y τ podemos asumir que $a = 1$. Se verifica fácilmente que este grupo es regular. Si B denota a la braza asociada a G, tenemos que $\sigma, \tau \in \ker \lambda$ y $\epsilon \in \mathrm{Fix}(B)$ y entonces $B = \ker \lambda + \mathrm{Fix}(B)$. Luego, se sigue la fórmula (4.12) por el lema 4.1.2. Por el corolario 3.1.2, tenemos que (4.12) define una bi-braza. □

De acuerdo con el teorema 4.2.6 existe una única braza no trivial de orden p^2q con $|\ker \lambda| = pq$. En consecuencia, tenemos la siguiente enumeración:

$\lvert\ker\lambda\rvert$	$\mathbb{Z}_p^2 \times \mathbb{Z}_q$	$\mathcal{G}_F$
p^2	-	1
pq	1	-
p^2q	1	-

Tabla 4.7: Enumeración de brazas de tipo $\mathbb{Z}_p^2 \times \mathbb{Z}_q$ para $p = -1 \pmod q$.

4.4. Brazas de orden p^2q con $q = 1 \pmod p$ y $q \neq 1 \pmod{p^2}$

En esta sección supondremos que $q = 1 \pmod p$ pero $q \neq 1 \pmod{p^2}$. Además tomaremos $p > 2$ y dejaremos el caso de $p = 2$ para la sección 4.6. Si notamos por r a un elemento fijo de orden p en $\mathbb{Z}_q^\times$, entonces los grupos no abelianos en las condiciones de esta sección son los siguientes, [14, Proposition 21.17]:

(i) $\mathbb{Z}_p \times (\mathbb{Z}_q \rtimes_r \mathbb{Z}_p) = \langle \sigma, \tau, \epsilon \,|\, \sigma^p = \tau^p = \epsilon^q = 1,\ [\epsilon, \tau] = [\tau, \sigma] = 1,\ \sigma\epsilon\sigma^{-1} = \epsilon^r \rangle$;

(ii) $\mathbb{Z}_q \rtimes_r \mathbb{Z}_{p^2} = \langle \sigma, \tau \,|\, \sigma^{p^2} = \tau^q = 1,\ \sigma\tau\sigma^{-1} = \tau^r \rangle$.

Resumimos en la siguiente tabla la enumeración de brazas de acuerdo con la clase de isomorfismo de sus estructuras multiplicativas y aditivas.

$+\backslash\circ$	$\mathbb{Z}_{p^2q}$	$\mathbb{Z}_q \rtimes_r \mathbb{Z}_{p^2}$	$\mathbb{Z}_p^2 \times \mathbb{Z}_q$	$\mathbb{Z}_p \times (\mathbb{Z}_q \rtimes_r \mathbb{Z}_p)$
$\mathbb{Z}_{p^2q}$	2	p	-	-
$\mathbb{Z}_p^2 \times \mathbb{Z}_q$	-	-	2	4

Tabla 4.8: Enumeración de brazas de orden p^2q con $q = 1 \pmod p$ y $q \neq 1 \pmod{p^2}$.

4.4.1. Brazas de tipo cíclico

Denotemos por A al grupo cíclico $\mathbb{Z}_{p^2q}$. Si G es un subgrupo regular de $\mathrm{Hol}(A)$ entonces $|\pi_2(G)| \in \{1, p, p^2\}$.

El grupo $\mathrm{Aut}\, A$ tiene un único p-subgrupo de Sylow que está generado por los automorfismos $\varphi_{p+1,1}$ y $\varphi_{1,r}$ y resulta ser elemental abeliano. Por lo tanto, los subgrupos de orden p de $\mathrm{Aut}\, A$ son

$$\langle \varphi_{p+1,1} \rangle \qquad \text{y} \qquad \langle \varphi_{jp+1,r} \rangle \tag{4.13}$$

donde $0 \leq j \leq p-1$.

Proposición 4.4.1. *Sea G un subgrupo regular de* $\mathrm{Hol}(A)$. *Entonces* $|\pi_2(G)| \neq p^2$.

Demostración. La imagen por π_2 de G es el único p-subgrupo de Sylow $\langle \varphi_{p+1,1},\ \varphi_{1,r} \rangle$ de $\mathrm{Aut}\, A$. El único subgrupo de A de orden q es $\langle \tau \rangle$, por lo cual G tiene la siguiente presentación estándar:

$$G = \langle \tau,\ \sigma^a \varphi_{p+1,1},\ \sigma^b \varphi_{1,r} \rangle.$$

El grupo $\pi_2(G)$ es elemental abeliano y por la condición (R) podemos ver que $a = b = 0 \pmod p$.

Por regularidad, $a, b \neq 0 \pmod{p^2}$. Sean $a = pa'$ y $b = pb'$ para ciertos elementos $1 \leq a', b' \leq p-1$. Luego $(\sigma^a \varphi_{p+1,1})^{-1} (\sigma^b \varphi_{1,r})^{\frac{a'}{b'}} = \varphi_{p+1,1}^{-1} \varphi_{1,r}^{\frac{a'}{b'}} \in G$ y entonces G no es regular, una contradicción.

□

Proposición 4.4.2. *Las brazas de tipo cíclico de orden p^2q con $|\ker\lambda| = pq$ son $B_{(j,k)} = (A, +, \circ)$ para $(j,k) \in \{(1,0)\} \cup \{(j,1) : 0 \leq j \leq p-1\}$ donde*

$$\binom{n}{m} + \binom{s}{t} = \binom{n+s}{m+t}, \qquad \binom{n}{m} \circ \binom{s}{t} = \binom{n + (jnp+1)s}{m + r^{kn}t}$$

para todos $0 \leq n, s \leq p^2 - 1$ y $0 \leq m, t \leq q-1$. En particular,

$$(B_{(j,k)}, \circ) \cong \begin{cases} \mathbb{Z}_{p^2q} & \text{si } (j,k) = (1,0), \\ \mathbb{Z}_q \rtimes_r \mathbb{Z}_{p^2}, & \text{en caso contrario.} \end{cases}$$

Demostración. Los grupos

$$H = \langle \sigma^p,\ \tau,\ \sigma\varphi_{p+1,1} \rangle \cong \mathbb{Z}_{p^2q}, \quad G_j = \langle \sigma^p,\ \tau,\ \sigma\varphi_{jp+1,r} \rangle \cong \mathbb{Z}_q \rtimes_r \mathbb{Z}_{p^2},$$

para $0 \leq j \leq p-1$ son subgrupos regulares y no son conjugados entre sí pues sus imágenes por π_2 no lo son.

Sea G un subgrupo regular con $|\pi_2(G)| = p$, entonces $\pi_2(G)$ es uno de los grupos de (4.13). Si $\pi_2(G) = \langle \varphi_{p+1,1} \rangle$ entonces podemos repetir el argumento del teorema 4.2.2 y conseguimos la braza asociada $B_{1,0}$.

Supongamos que $\pi_2(G) = \langle \varphi_{jp+1,r} \rangle$ para cierto $0 \leq j \leq p-1$. Luego, el núcleo de π_2 es el único subgrupo de orden pq, digamos $\langle \sigma^p, \tau \rangle$ y entonces G tiene la siguiente presentación estándar:

$$G = \langle \sigma^p,\ \tau,\ \sigma^a\varphi_{jp+1,r} \rangle,$$

donde $1 \leq a \leq p-1$ pues G es regular. Entonces, G es conjugado a G_j por $\varphi_{a^{-1},1}$. Sea $B_{j,1}$ la braza asociada a G_j.

Luego, como $\langle \tau, \sigma^p \rangle \leq \ker \pi_2$ y $\underbrace{\sigma \circ \sigma \circ \ldots \circ \sigma}_{n} = \sigma^{\frac{n(n-1)p}{2}+n} = \sigma^{\frac{n(n-1)p}{2}} \circ \sigma^n$ se tiene que

$$\lambda_{\sigma^n\tau^m} = \lambda_{\tau^m \circ \sigma^n} = \lambda_{\sigma^n} = \lambda_\sigma^n = \varphi_{jp+1,r}^n$$

de lo cual se deduce la fórmula del enunciado. □

Resumiendo, los resultados de esta subsección aparecen en la siguiente tabla:

$\ker\lambda$	$\mathbb{Z}_{p^2q}$	$\mathbb{Z}_q \rtimes_r \mathbb{Z}_{p^2}$
pq	1	p
p^2q	1	-

Tabla 4.9: Enumeración de las brazas de tipo cíclico de orden p^2q con $q = 1 \pmod p$ y $q \neq 1 \pmod{p^2}$.

4.4.2. Brazas de tipo $\mathbb{Z}_p^2 \times \mathbb{Z}_q$

En esta sección denotaremos por A al grupo $\mathbb{Z}_p^2 \times \mathbb{Z}_q$ y por C a la matriz definida en la observación 4.2.5.

Proposición 4.4.3. *Las brazas de tipo A con* $|\ker\lambda| = pq$ *son* $(B_{i,j}, +, \circ)$ *para* $0 \le i, j \le 1$ *y* $(i,j) \neq (0,0)$*, donde*

$$\begin{pmatrix} n \\ m \\ l \end{pmatrix} + \begin{pmatrix} s \\ t \\ u \end{pmatrix} = \begin{pmatrix} n+s \\ m+t \\ l+u \end{pmatrix}, \qquad \begin{pmatrix} n \\ m \\ l \end{pmatrix} \circ \begin{pmatrix} s \\ t \\ u \end{pmatrix} = \begin{pmatrix} n+s+jmt \\ m+t \\ l+r^{im}u \end{pmatrix},$$

para todos $0 \le n, m, s, t \le p-1$ *y* $0 \le l, u \le q-1$*. En particular,*

$$(B_{i,j}, \circ) \cong \begin{cases} \mathbb{Z}_p^2 \times \mathbb{Z}_q, & \text{si } (i,j) = (0,1), \\ \mathbb{Z}_p \times (\mathbb{Z}_q \rtimes_r \mathbb{Z}_p), & \text{en caso contrario.} \end{cases}$$

Demostración. Sea $G \le \mathrm{Hol}(A)$ un subgrupo regular con $|\pi_2(G)| = p$. Luego, salvo conjugación, la imagen $\pi_2(G)$ está generada por r^iC^j, para ciertos $i, j \in \{0,1\}$ con $(i,j) \neq (0,0)$. El núcleo de $\pi_2|_G$ tiene orden pq, por lo cual $\ker\pi_2|_G = \langle \epsilon, v\rangle$ para algún $v \in \langle\sigma,\tau\rangle$. En consecuencia, tenemos la siguiente presentación estándar:

$$G_{i,j} = \langle v,\ \epsilon,\ ur^iC^j\rangle,$$

para algún $u \in \langle\sigma,\tau\rangle$. Si $(i,j) = (0,1)$ podemos argumentar como en la demostración del teorema 4.2.6 y conseguimos la fórmula correspondiente.

Si $(i,j) = (1,0)$ entonces, salvo conjugación por un elemento de $GL_2(p)$, podemos suponer que $v = \sigma$ y $u = \tau$.

Si consideramos el caso $(i,j) = (1,1)$, por la condición (K) tenemos $v \in \langle\sigma\rangle$ y entonces

$$G_{1,1} = \langle\sigma,\ \epsilon,\ \tau^a rC\rangle,$$

con $a \neq 0$. Podemos suponer que $a = 1$ conjugando por $a^{-1}I$ si fuera necesario.

Sea $B_{i,j}$ la braza asociada a $G_{i,j}$. En los dos últimos casos, se cumple que $\lambda_{\sigma^n\tau^m\epsilon^l} = \lambda_{\tau^m} = \lambda_\tau^m$ pues $\sigma, \epsilon \in \ker\pi_2$ y $\lambda_\tau(\tau) = \tau$ (mód $\langle\sigma\rangle$). Y esto concluye la prueba.

□

Proposición 4.4.4. *Sea w un no-residuo cuadrático fijo módulo p. Las brazas de tipo A con* $|\ker\lambda| = q$ *son* $(B_s, +, \circ)$ *para* $s \in \{1, w\}$*, donde*

$$\begin{pmatrix} n \\ m \\ l \end{pmatrix} + \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} n+x \\ m+y \\ l+z \end{pmatrix}, \quad \begin{pmatrix} n \\ m \\ l \end{pmatrix} \circ \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} n+x+yms^{-1} \\ m+y \\ l+zr^{n-m\frac{m-s}{2s}} \end{pmatrix},$$

para todos $0 \le n, m, x, y \le p-1$ *y* $0 \le l, z \le q-1$.

En particular, $(B_s, \circ) \cong \mathbb{Z}_p \times (\mathbb{Z}_q \rtimes_r \mathbb{Z}_p)$.

Demostración. Los grupos

$$G_s = \langle \epsilon,\ \tau^s C,\ \sigma r\rangle \cong \mathbb{Z}_p \times (\mathbb{Z}_q \rtimes_r \mathbb{Z}_p)$$

con $s \in \{1, w\}$ son subgrupos regulares de $\mathrm{Hol}(A)$ con $|\pi_2(G_s)| = p^2$ y no son conjugados entre sí. En efecto, si fueran conjugados por un cierto h, entonces h sería un elemento de $N_{\mathrm{Aut}\,A}(C)$, el normalizador de C en $\mathrm{Aut}\,A$, digamos que

$$h = \begin{bmatrix} x & y \\ 0 & z \end{bmatrix} r^a.$$

Luego, tenemos que $h\tau C h^{-1} = \sigma^y \tau^z C^{\frac{x}{z}}$ y $h\sigma r h^{-1} = \sigma^x r$ pertenece a G_w. Entonces $x = 1$ y por lo tanto $\sigma^y \tau^z C^{\frac{1}{z}} = (\tau^w C)^{\frac{1}{z}}$. Comparando las potencias de τ a ambos lados, tenemos $w = z^2$, una contradicción.

Sea $G \leq \mathrm{Hol}(A)$ un subgrupo regular tal que $|\pi_2(G)| = p^2$. Entonces, salvo conjugación, tenemos $\pi_2(G) = \langle C, r\rangle$. Por lo tanto, G tiene la siguiente presentación estándar:

$$G = \langle \epsilon,\ uC,\ vr\rangle,$$

para ciertos $u, v \in \langle \sigma, \tau\rangle$. Por la condición (R), los dos últimos generadores conmutan módulo $\langle \epsilon\rangle$ y esto implica que $v \in \langle \sigma\rangle$. Entonces G es de la forma

$$G_u = \langle \epsilon,\ uC,\ \sigma^m r\rangle$$

donde $m \neq 0$. Podemos asumir que $m = 1$ conjugando por $m^{-1}I$ si fuera necesario.

Supongamos que $u = \sigma^s$. Como G_u es regular, $s \neq 0$ y entonces tenemos que $(\sigma^s C)^{-s^{-1}} \sigma r = C^{-s^{-1}} r \in G$. Por el lema 4.1.3, G_u no sería regular, una contracción.

Si $u = \sigma^s \tau^t$ para algún $t \neq 0$, conjugando por $C^{-\frac{s}{t}}$ podemos asumir que $u = \tau^t$. Si $t = z^2$ para algún z entonces $G_{\tau^{z^2}}$ es conjugado de G_1 por h que está dado por

$$h = \begin{bmatrix} 1 & 2^{-1}(1 - z^{-1}) \\ 0 & z^{-1} \end{bmatrix}.$$

En caso contrario, podemos escribir $t = wz^2$ para cierto z donde w es un no-residuo cuadrático módulo p. En consecuencia, $hG_{\tau^t}h^{-1} = G_w$ para el mismo h de arriba.

Sea B_s la braza asociada a G_s. Entonces $\lambda_\sigma|_{\langle\sigma,\tau\rangle} = \mathrm{id}|_{\langle\sigma,\tau\rangle}$ y por lo tanto $\lambda_{\sigma^n} = \lambda_\sigma^n$ de acuerdo con el lema 4.1.2. Más aún, tenemos que

$$\begin{aligned} \underbrace{\tau^s \circ \cdots \circ \tau^s}_{m} = \sigma^{s\frac{m(m-1)}{2}} \tau^{ms} = \sigma^{s\frac{m(m-1)}{2}} \circ \tau^{ms} \\ \iff \tau^m = \tau^{\frac{m}{s}s} = \left(\sigma^{\frac{m(m-s)}{2s}}\right)' \circ \underbrace{\tau^s \circ \cdots \circ \tau^s}_{\frac{m}{s}} \end{aligned} \tag{4.14}$$

para todo $m \in \mathbb{N}$. Luego, utilizando (4.14) y el hecho de que $\lambda_\sigma(\tau) = \tau$ se sigue que

$$\begin{aligned} \lambda_{\epsilon^l \sigma^n \tau^m} &= \lambda_{\epsilon^l \circ \sigma^n \circ \tau^m} = \lambda_\sigma^n \lambda_{\tau^m} \\ &= r^n r^{-\frac{m(m-s)}{2s}} C^{\frac{m}{s}} = r^{n - \frac{m(m-s)}{2s}} C^{\frac{m}{s}}. \end{aligned}$$

Finalmente, se deduce la fórmula para la operación $\circ$. □

Resumimos el contenido de esta subsección en la siguiente tabla:

$\lvert\ker\lambda\rvert$	$\mathbb{Z}_p^2 \times \mathbb{Z}_q$	$\mathbb{Z}_p \times (\mathbb{Z}_q \rtimes_r \mathbb{Z}_p)$
q	-	2
pq	1	2
p^2q	1	-

Tabla 4.10: Enumeración de las brazas de tipo $\mathbb{Z}_p^2 \times \mathbb{Z}_q$ de orden p^2q para $q = 1 \pmod p$ y $q \neq 1 \pmod{p^2}$.

4.5. Brazas de orden p^2q con $q = 1 \pmod{p^2}$

En esta sección asumimos que $q = 1 \pmod{p^2}$ donde p es un primo impar. Fijamos un elemento h de orden p^2 en $\mathbb{Z}_q^\times$. Bajo estas condiciones debemos considerar los siguientes grupos de orden p^2q, [14, Proposition 21.17]:

(i) $\mathbb{Z}_p \times (\mathbb{Z}_q \rtimes_{h^p} \mathbb{Z}_p) = \langle \sigma, \tau, \epsilon \,|\, \sigma^p = \tau^p = \epsilon^q = 1,\ [\epsilon, \tau] = [\tau, \sigma] = 1,\ \sigma\epsilon\sigma^{-1} = \epsilon^{h^p} \rangle$,

(ii) $\mathbb{Z}_q \rtimes_{h^p} \mathbb{Z}_{p^2} = \langle \sigma, \tau \,|\, \tau^q = \sigma^{p^2} = 1,\ \sigma\tau\sigma^{-1} = \tau^{h^p} \rangle$,

(iii) $\mathbb{Z}_q \rtimes_h \mathbb{Z}_{p^2} = \langle \sigma, \tau \,|\, \tau^q = \sigma^{p^2} = 1,\ \sigma\tau\sigma^{-1} = \tau^h \rangle$.

La siguiente tabla resume la cantidad total de brazas según las clases de isomorfismo de sus grupos aditivos y multiplicativos bajo las condiciones de esta sección.

$+\backslash\circ$	$\mathbb{Z}_{p^2q}$	$\mathbb{Z}_q \rtimes_{h^p} \mathbb{Z}_{p^2}$	$\mathbb{Z}_q \rtimes_h \mathbb{Z}_{p^2}$	$\mathbb{Z}_p^2 \times \mathbb{Z}_q$	$\mathbb{Z}_p \times (\mathbb{Z}_q \rtimes_{h^p} \mathbb{Z}_p)$
$\mathbb{Z}_{p^2q}$	2	p	p	-	-
$\mathbb{Z}_p^2 \times \mathbb{Z}_q$	-	-	-	2	4

Tabla 4.11: Enumeración de brazas de orden p^2q con $q = 1 \pmod{p^2}$.

4.5.1. Brazas de tipo cíclico

En esta sección consideraremos el grupo cíclico $\mathbb{Z}_{p^2q}$ de orden p^2q. El orden de la imagen por π_2 de un subgrupo regular de $\operatorname{Aut}\mathbb{Z}_{p^2q}$ divide a p^2.

Lema 4.5.1. *Los subgrupos de orden p^2 $\operatorname{Aut}\mathbb{Z}_{p^2q}$ son*

$$H_j = \langle \varphi_{jp+1,h} \rangle \quad y \quad T = \langle \varphi_{p+1,1},\ \varphi_{1,h^p} \rangle$$

para $0 \leq j \leq p-1$.

Demostración. Todo subgrupo de orden p^2 en $\operatorname{Aut}\mathbb{Z}_{p^2q}$ está incluido en el subgrupo de los elementos de orden a lo sumo p^2 de $\operatorname{Aut}A$, que está generado por $\varphi_{p+1,1}$ y $\varphi_{1,h}$ y es isomorfo a $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$. Por [66, Theorem 3.3], el grupo $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$ tiene $p+1$ subgrupos de orden p^2. Los subgrupos $\langle \varphi_{p+1,1},\ \varphi_{1,h^p} \rangle$ y $\langle \varphi_{jp+1,h} \rangle$ con $0 \leq j \leq p-1$ son en total $p+1$ subgrupos distintos de orden p^2. □

Para la siguiente proposición necesitaremos de un lema.

Lema 4.5.2. *La función*

$$f_j : \mathbb{Z}_{p^2} \longrightarrow \mathbb{Z}_{p^2}, \quad m \mapsto \frac{m(m-1)}{2} jp + m$$

es biyectiva para cualquier $0 \leq j \leq p-1$.

Demostración. Claramente $f_j(m) = m \pmod{p}$ y se puede probar por inducción que $f_j(m + kp) = f_j(m) + kp$. Como todo elemento de $\mathbb{Z}_{p^2}$ es de la forma $m + kp$ para m, k adecuados entonces f_j es sobreyectiva. □

Proposición 4.5.3. *Las brazas de tipo cíclico con* $|\ker \lambda| = q$ *son* $(B_j, +, \circ)$ *con* $0 \leq j \leq p-1$ *donde*

$$\binom{n}{m} + \binom{x}{y} = \binom{n+x}{m+y}, \quad \binom{n}{m} \circ \binom{x}{y} = \binom{n + \left(f_j^{-1}(n)pj + 1\right)x}{m + h^{f_j^{-1}(n)} y},$$

para todos $0 \leq n, x \leq p-1$ *y* $0 \leq m, y \leq q-1$. *En particular,* $(B_j, \circ) \cong \mathbb{Z}_q \rtimes_h \mathbb{Z}_{p^2}$.

Demostración. Los grupos

$$G_j = \langle \tau,\ \sigma\varphi_{jp+1,h} \rangle \cong \mathbb{Z}_q \rtimes_h \mathbb{Z}_{p^2},$$

con $0 \leq j \leq p-1$ son regulares y no son conjugados entre sí pues sus imágenes por π_2 no son conjugadas entre sí. Por el lema 4.5.1, tenemos los siguientes casos:

(i) $\pi_2(G) = T$: de forma análoga a la proposición 4.4.1, podemos mostrar que no hay subgrupos regulares que cumplan con esta condición.

(ii) $\pi_2(G) = H_j$: en este caso, una presentación estándar de G es

$$G = \langle \tau,\ \sigma^a \tau^b \varphi_{jp+1,h} \rangle = \langle \tau,\ \sigma^a \varphi_{jp+1,h} \rangle,$$

donde $a \neq 0$ pues G es regular. Entonces G es conjugado de G_j por $\varphi_{a^{-1},1}$.

Sea $(B_j, +, \circ)$ la braza asociada a G_j, entonces

$$\underbrace{\sigma \circ \ldots \circ \sigma}_{n} = \sigma^{f_j(n)},$$

con f_j como en el lema 4.5.2. Luego $\lambda_{\sigma^n \tau^m} = \lambda_{\tau^m \circ \sigma^n} = \lambda_\sigma^{f_j^{-1}(n)}$ y se sigue la fórmula. □

Para el caso $|\pi_2(G)| = p$, los subgrupos de orden p de $\operatorname{Aut} A$ son los mismos de la subsección 4.4.1 por lo cual podemos argumentar igual que en la proposición 4.4.2 y conseguimos $p + 1$ brazas de tipo A con $|\ker \lambda| = pq$.

Resumimos el contenido de esta subsección en la siguiente tabla:

$\lvert\ker\lambda\rvert$	$\mathbb{Z}_{p^2q}$	$\mathbb{Z}_q \rtimes_h \mathbb{Z}_{p^2}$	$\mathbb{Z}_q \rtimes_{h^p} \mathbb{Z}_{p^2}$
q	-	p	-
pq	1	-	p
p^2q	1	-	-

Tabla 4.12: Enumeración de brazas de tipo cíclico de orden p^2q con $q = 1 \pmod{p^2}$.

4.5.2. Brazas de tipo $\mathbb{Z}_p^2 \times \mathbb{Z}_q$

En esta sección denotaremos por A al grupo $\mathbb{Z}_p^2 \times \mathbb{Z}_q$. El orden del núcleo de λ de brazas no triviales de tipo A es o bien q o bien pq. Las clases de conjugación de los subgrupos de orden p de $\operatorname{Aut} A$ son los mismos del caso $q = 1 \pmod{p}$ y entonces, si $\lvert\ker\lambda\rvert = pq$ estamos en la misma situación de la proposición 4.4.3.

Salvo conjugación, los subgrupos de orden p^2 de $\operatorname{Aut} A$ son $\langle C, h^p\rangle$ y $\langle C^l h\rangle$ donde $l = 0, 1$ y C como en la observación 4.2.5. Si G es un subgrupo regular de $\operatorname{Hol}(A)$ con $\pi_2(G) = \langle C^l h\rangle$ entonces

$$G = \langle \epsilon,\ vC^l h\rangle$$

para cierto $v = \sigma^a\tau^b$. Entonces

$$(vC^l h)^p = vC^l(v)C^{2l}(v)\cdots C^{(p-1)l}(v)C^{pl}h^p = h^p \in G.$$

Luego, por el lema 4.1.3 G no es regular. Por otro lado, si $\pi_2(G) = \langle C, h^p\rangle$, podemos argumentar como en la proposición 4.4.4 y por lo tanto tenemos una descripción completa de las brazas de tipo A con $\lvert\ker\lambda\rvert = q$.

En consecuencia, la enumeración de brazas de tipo A de orden p^2q para el caso $q = 1 \pmod{p^2}$ es la de la tabla 4.10.

4.6. Brazas de orden $4q$ con $q = 1 \pmod 2$ y $q \neq 1 \pmod 4$

Consideramos aquí el caso de los números primos $q > 3$.

Los resultados de esta sección y de la sección 4.7 están contenidos en el trabajo de Dietzel (véase [29, Theorem 5]). Asumiremos que $q = 1 \pmod 2$ (por ser un número primo impar) pero $q \neq 1 \pmod 4$. De acuerdo con [46, Proposition 2.1], los grupos no abelianos de orden $4q$ con $q > 3$ son:

(i) $\mathbb{Z}_2 \times (\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_2)$, el grupo diedral de orden $4q$; y

(ii) $\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_4 = \langle \sigma, \tau \mid \sigma^4 = \tau^q = 1,\ \sigma\tau\sigma^{-1} = \tau^{-1}\rangle$.

Para $q = 3$, los grupos no abelianos de orden 12 son $\mathbb{Z}_2 \times (\mathbb{Z}_3 \rtimes_{-1} \mathbb{Z}_2)$, $\mathbb{Z}_3 \rtimes_{-1} \mathbb{Z}_4$ y A_4, el grupo alternado en 4 letras. Las brazas torcidas correspondientes se encuentran explícitamente en el paquete *YangBaxter* de GAP, [69], por lo cual hemos decidido dejar de lado este caso especial.

La enumeración de brazas de esta sección se encuentra resumida en la siguiente tabla.

$+\backslash\circ$	$\mathbb{Z}_{4q}$	$\mathbb{Z}_2^2 \times \mathbb{Z}_q$	$\mathbb{Z}_2 \times (\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_2)$	$\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_4$
$\mathbb{Z}_{4q}$	1	1	2	1
$\mathbb{Z}_2^2 \times \mathbb{Z}_q$	1	1	1	1

Tabla 4.13: Enumeración de brazas de orden $4q$ con $q = 1 \pmod 2$ y $q \neq 1 \pmod 4$.

4.6.1. Brazas de tipo cíclico

Denotemos por A al grupo cíclico de orden $4q$. Como $\operatorname{Aut} A$ tiene orden $2(q-1)$, si G es un subgrupo regular de $\operatorname{Hol}(A)$ entonces $|\pi_2(G)|$ divide a 4. Su grupo de automorfismos contiene un único subgrupo de orden 4 que está generado por $\varphi_{-1,1}$ y $\varphi_{1,-1}$ y es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$. Luego, tiene tres subgrupos no conjugados entre sí de orden 2, generados por $\varphi_{(-1)^i,(-1)^j}$ con $(i,j) \in \{(1,0),(1,1),(0,1)\}$.

Proposición 4.6.1. *Las brazas de orden $4q$ con $|\ker \lambda| = 2q$ son $(B_{i,j}, +, \circ)$ para $(i,j) \in \{(1,0),(1,1),(0,1)\}$ donde*

$$\binom{n}{m} + \binom{x}{y} = \binom{n+x}{m+y}, \quad \binom{n}{m} \circ \binom{x}{y} = \binom{n+(-1)^{jm}x}{m+(-1)^{im}y}$$

para todos $0 \leq n, x \leq q-1$ y $0 \leq m, y \leq 3$. En particular,

$$(B_{i,j}, \circ) \cong \begin{cases} \mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_4, & \text{si } (i,j) = (0,1), \\ \mathbb{Z}_2 \times (\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_2), & \text{si } (i,j) = (1,1), \\ \mathbb{Z}_2^2 \times \mathbb{Z}_q, & \text{si } (i,j) = (1,0). \end{cases}$$

Demostración. Los grupos

$$G_{i,j} = \langle \tau,\, \sigma^2,\, \sigma\varphi_{(-1)^i,(-1)^j} \rangle \cong \begin{cases} \mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_4, & \text{si } (i,j) = (0,1), \\ \mathbb{Z}_2 \times (\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_2), & \text{si } (i,j) = (1,1), \\ \mathbb{Z}_2^2 \times \mathbb{Z}_q, & \text{si } (i,j) = (1,0) \end{cases}$$

para $(i,j) \in I = \{(1,0),(1,1),(0,1)\}$ son regulares y no son conjugados entre sí puesto que no son isomorfos entre sí.

Como mencionamos anteriormente, si G es un subgrupo regular entonces tenemos que $\pi_2(G) = \langle \varphi_{(-1)^i,(-1)^j} \rangle$ para cierto $(i,j) \in I$. Supongamos que $\pi_2(G)$ está generado por $\varphi_{1,-1}$, luego G tiene la presentación estándar:

$$G = \langle \tau,\ \sigma^2,\ \sigma^a\varphi_{1,-1} \rangle.$$

Dado que G es regular tenemos que $a \neq 0$ por lo cual podemos asumir que $a = 1$ y entonces $G = G_{0,1}$. Como $\tau \in \ker \pi_2$ y $\varphi_{1,-1}(\sigma) = \sigma$, la braza $B_{0,1}$ asociada a

$G_{0,1}$ se puede escribir como $\ker\lambda + \mathrm{Fix}(B_{0,1})$. Gracias al lema 4.1.2, tenemos que $\lambda_{\tau^n\sigma^m} = \lambda_{\tau^n\circ\sigma^m} = \lambda_{\sigma^m} = \lambda_\sigma^m$. De lo cual se sigue la fórmula para $B_{0,1}$.

Los otros dos casos son completamente análogos por lo cual omitimos los cálculos. □

Lema 4.6.2. *La única braza de tipo cíclico con* $|\ker\lambda| = q$ *es* $(B, +, \circ)$ *con*

$$\binom{n}{m} + \binom{x}{y} = \binom{n+x}{m+y}, \qquad \binom{n}{m} \circ \binom{x}{y} = \binom{n + (-1)^{\frac{m(m-1)}{2}} x}{m + (-1)^m y}$$

para todos $0 \le n, x \le q-1$ *y* $0 \le m, y \le 3$. *En particular,* $(B, \circ) \cong \mathbb{Z}_2 \times (\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_2)$.

Demostración. El grupo

$$H = \langle \tau,\ \sigma^2\varphi_{1,-1},\ \sigma\varphi_{-1,1} \rangle \cong \mathbb{Z}_2 \times (\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_2)$$

es regular. Sea G un subgrupo regular de $\mathrm{Hol}(A)$ con $|\pi_2(G)| = 4$. Veamos que necesariamente es un conjugado de H. Como el único subgrupo de orden q de A está generado por τ tenemos que G tiene la siguiente presentación estándar

$$G = \langle \tau,\ \sigma^a\varphi_{1,-1},\ \sigma^b\varphi_{-1,1} \rangle$$

para ciertos $1 \le a, b \le 3$. Por las condiciones (K) tenemos que $a = 2$. Si $b = 2$ entonces $\sigma^2\varphi_{1,-1}\sigma^2\varphi_{-1,1} = \varphi_{1,-1}\varphi_{-1,1} \in G$ y entonces G no es regular. Luego, salvo conjugación por $\varphi_{-1,1}$ podemos suponer que $b = 1$ y entonces G es un conjugado de H. Las fórmulas del enunciado definen una braza con las propiedades deseadas y por lo tanto es isomorfa a la braza asociada al único subgrupo regular G con $|\pi_2(G)| = 4$. □

Tenemos la siguiente tabla resumiendo las brazas de tipo cíclico:

$\ker\lambda$	$\mathbb{Z}_{4q}$	$\mathbb{Z}_2^2 \times \mathbb{Z}_q$	$\mathbb{Z}_2 \times (\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_2)$	$\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_4$
q	-	-	1	-
$2q$	-	1	1	1
$4q$	1	-	-	-

Tabla 4.14: Enumeración de brazas de tipo cíclico de orden $4q$ con $q = 1 \pmod 2$ y $q \neq 1 \pmod 4$.

4.6.2. Brazas de tipo $\mathbb{Z}_2^2 \times \mathbb{Z}_q$

En esta subsección, A denotará al grupo abeliano $\mathbb{Z}_2^2 \times \mathbb{Z}_q$. Salvo conjugación, $\mathrm{Aut}\, A$ tiene un único subgrupo de orden 4 que resulta isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$ y está generado por

$$C = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

y $\eta = -1$. Luego, tenemos tres posibles subgrupos de orden 2 salvo conjugación.

Podemos decir que son los subgrupos generados por $C^i\eta^j$ para algún par de índices $(i, j) \in \{(1, 0), (1, 1), (0, 1)$.

Lema 4.6.3. *Si G es un subgrupo regular de* $\mathrm{Hol}(A)$ *entonces* $|\pi_2(G)| \neq 4$.

Demostración. Por la discusión previa y el hecho de que A tiene un único subgrupo de orden q, digamos $\langle\epsilon\rangle$, entonces G tiene la siguiente presentación estándar:

$$G = \langle \epsilon,\ \sigma^a\tau^b C,\ \sigma^c\tau^d\eta\rangle$$

para ciertos $0 \leq a, b, c, d \leq 1$. Por las condiciones (K) $(\sigma^a\tau^b C)^2, [\sigma^a\tau^b C, \sigma^c\tau^d\eta] \in \langle\epsilon\rangle$ entonces tenemos que $b = d = 0$ y por lo tanto $a, c \neq 0$. Finalmente, tenemos que $(\sigma C)^{-\frac{c}{a}}\sigma^c\eta = C^{-\frac{c}{a}}\eta \in G$ por lo cual G no es regular. □

Proposición 4.6.4. *Las brazas de orden $4q$ con $|\ker\lambda| = 2q$ son $(B_{i,j}, +, \circ)$ para $(i,j) \in \{(1,0),(0,1),(1,1)\}$, donde*

$$\begin{pmatrix} n \\ m \\ l \end{pmatrix} + \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} n+x \\ m+y \\ l+z \end{pmatrix}, \qquad \begin{pmatrix} n \\ m \\ l \end{pmatrix} \circ \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} n+(-1)^{il}x \\ m+y+jlz \\ l+z \end{pmatrix}$$

para todos $0 \leq n, x \leq q-1$ y $0 \leq m, l, y, z \leq 1$. En particular,

$$(B_{i,j}, \circ) \cong \begin{cases} \mathbb{Z}_2 \times (\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_2), & si\ (i,j) = (1,0), \\ \mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_4, & si\ (i,j) = (1,1), \\ \mathbb{Z}_{4q}, & si\ (i,j) = (0,1). \end{cases}$$

Demostración. Los grupos

$$G_{i,j} = \langle \sigma,\ \epsilon,\ \tau\eta^i C^j\rangle \cong \begin{cases} \mathbb{Z}_2 \times (\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_2), & \text{si } (i,j) = (1,0), \\ \mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_4, & \text{si } (i,j) = (1,1), \\ \mathbb{Z}_{4q}, & \text{si } (i,j) = (0,1) \end{cases}$$

para $(i,j) \in \{(1,0),(0,1),(1,1)\}$ son regulares y no son conjugados entre sí puesto que ni siquiera son isomorfos.

Sea G un subgrupo regular de $\mathrm{Hol}(A)$ con $|\pi_2(G)| = 2$ y el núcleo de orden $2q$. En este caso, tendrá la forma $\langle\epsilon, v\rangle$ para cierto $v \in \langle\sigma,\tau\rangle$.

Supongamos que $\pi_2(G) = \langle\eta\rangle$. Como todo elemento de $GL_2(2)$ centraliza a η podemos asumir $v = \sigma$ salvo conjugación. Luego G es un conjugado de $G_{1,0}$. Sea $B_{1,0}$ la braza asociada a $G_{1,0}$. Como $\langle\sigma,\epsilon\rangle \subseteq \ker\lambda$ y $\langle\tau\rangle \subseteq \mathrm{Fix}(B_{1,0})$, tenemos que $B_{1,0} = \ker\lambda + \mathrm{Fix}(B_{1,0})$. Luego, la fórmula se sigue del lema 4.1.2.

Para el caso $\pi_2(G) = \langle C\rangle$, conjugando por elementos de $N_{GL_2(p)}(C)$ podemos suponer que $v = \sigma, \tau$. La primera opción nos lleva a $G_{0,1}$ y la segunda nos da la presentación estándar

$$G = \langle \tau,\ \epsilon,\ \sigma C\rangle.$$

La condición (K) nos lleva a una contradicción.

Si $\pi_2(G) = \langle C, \eta\rangle$ podemos argumentar igual y llegamos a las fórmulas por el mismo argumento del primer caso. □

La siguiente tabla resume los resultados de esta subsección.

$\ker\lambda$	$\mathbb{Z}_{4q}$	$\mathbb{Z}_2^2\times\mathbb{Z}_q$	$\mathbb{Z}_2\times(\mathbb{Z}_q\rtimes_{-1}\mathbb{Z}_2)$	$\mathbb{Z}_q\rtimes_{-1}\mathbb{Z}_4$
$2q$	1	-	1	1
$4q$	-	1	-	-

Tabla 4.15: Enumeración de las brazas de orden $4q$ de tipo $\mathbb{Z}_2^2\times\mathbb{Z}_q$.

4.7. Brazas de orden $4q$ con $q = 1 \pmod 4$

En esta sección consideramos las brazas de orden $4q$ con $q = 1 \pmod 4$. Los grupos no abelianos de orden $4q$ son los mismos de la sección 4.6 pero se agrega uno extra:

$$\mathbb{Z}_q\rtimes_\xi\mathbb{Z}_4=\langle\sigma,\tau\,|\,\sigma^4=\tau^q=1,\ \sigma\tau\sigma^{-1}=\tau^\xi\rangle$$

donde ξ es un elemento de orden 4 en $\mathbb{Z}_q^\times$, [46, Proposition 2.1].

La siguiente tabla resume las brazas que obtendremos en esta sección.

$+\backslash\circ$	$\mathbb{Z}_{4q}$	$\mathbb{Z}_2^2\times\mathbb{Z}_q$	$\mathbb{Z}_2\times(\mathbb{Z}_q\rtimes_{-1}\mathbb{Z}_2)$	$\mathbb{Z}_q\rtimes_{-1}\mathbb{Z}_4$	$\mathbb{Z}_q\rtimes_\xi\mathbb{Z}_4$
$\mathbb{Z}_{4q}$	1	1	2	1	1
$\mathbb{Z}_2^2\times\mathbb{Z}_q$	1	1	1	1	1

Tabla 4.16: Enumeración de brazas de orden $4q$ con $q = 1 \pmod 4$.

4.7.1. Brazas de tipo cíclico

En esta subsección denotaremos por A al grupo cíclico de orden $4q$. El grupo de automorfismos de A tiene orden $2(q-1)$, por lo tanto el orden de la imagen por π_2 de cualquier subgrupo regular divide a 4. El grupo $\mathbb{Z}_q^\times$ contiene un elemento ξ de orden 4 pues $q = 1 \pmod 4$ y claramente $\xi^2 = -1$.

El subgrupo de $\operatorname{Aut}A\cong\mathbb{Z}_2\times\mathbb{Z}_q^\times$ que contiene a los elementos de orden a lo sumo 4 está generado por $\varphi_{-1,1}$ y $\varphi_{1,\xi}$ y resulta isomorfo a $\mathbb{Z}_2\times\mathbb{Z}_4$. El subgrupo de los elementos de orden 2 de $\operatorname{Aut}A$ está generado por $\varphi_{-1,1}$ y $\varphi_{1,-1}$, por lo cual es el mismo que consideramos en la subsección 4.6.1, y entonces las brazas con $|\ker\lambda| = 2q$ son como en el lema 4.6.1.

Por otro lado, tenemos tres subgrupos de $\operatorname{Aut}A$ de orden 4: $\langle\varphi_{1,-1},\varphi_{-1,1}\rangle$, $\langle\varphi_{1,\xi}\rangle$ y $\langle\varphi_{-1,\xi}\rangle$.

Lema 4.7.1. *Las brazas de orden $4q$ con $|\ker\lambda| = q$ son $(B_i,+,\circ)$ para $i = 1,2$ donde*

$$B_1:\quad \binom{n}{m}+\binom{x}{y}=\binom{n+x}{m+y},\qquad \binom{n}{m}\circ\binom{x}{y}=\binom{n+(-1)^{\frac{m(m-1)}{2}}x}{m+(-1)^m y},$$

$$B_2:\quad \binom{n}{m}+\binom{x}{y}=\binom{n+x}{m+y},\qquad \binom{n}{m}\circ\binom{x}{y}=\binom{n+\xi^m x}{m+y}$$

para todos $0 \leq n, x \leq q-1$ *y* $0 \leq m, y \leq 3$. *En particular* $(B_2, +, \circ)$ *es una bi-braza y tenemos*

$$(B_1, \circ) \cong \mathbb{Z}_2 \times (\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_2) \qquad y \qquad (B_2, \circ) \cong \mathbb{Z}_q \rtimes_{\xi} \mathbb{Z}_4.$$

Demostración. Los grupos

$$G_1 = \langle \tau,\ \sigma^2\varphi_{1,-1},\ \sigma\varphi_{-1,1} \rangle \cong \mathbb{Z}_2 \times (\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_2) \qquad \text{y} \qquad G_2 = \langle \tau,\ \sigma\varphi_{1,\xi} \rangle \cong \mathbb{Z}_q \rtimes_{\xi} \mathbb{Z}_4$$

son regulares y no son sonjugados entre sí dado que no son isomorfos. Sea G un subgrupo regular de $\mathrm{Hol}(A)$ con $|\pi_2(G)| = 4$. El grupo A tiene un único subgrupo de orden q que está generado por τ. Tenemos tres casos.

Si $\pi_2(G) = \langle \varphi_{1,-1},\ \varphi_{-1,1} \rangle$, entonces aplicamos el lema 4.6.2 y conseguimos la braza B_1. Si $\pi_2(G) = \langle \varphi_{1,\xi} \rangle$ entonces una presentación estándar para G es G_2, la braza asociada es B_2 y además B_2 es una bi-braza gracias a la proposición 3.1.1. Si $\pi_2(G) = \langle \varphi_{-1,\xi} \rangle$ entonces una presentación estándar para G es

$$G = \langle \tau,\ \sigma\varphi_{-1,\xi} \rangle.$$

Como $(\sigma\varphi_{-1,\xi})^2 = \varphi_{-1,\xi}^2 = \varphi_{1,-1} \in G$, entonces G no es regular por el lema 4.1.3. □

La siguiente tabla resume las brazas obtenidas en esta subsección.

$\ker\lambda$	$\mathbb{Z}_{4q}$	$\mathbb{Z}_2^2 \times \mathbb{Z}_q$	$\mathbb{Z}_2 \times (\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_2)$	$\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_4$	$\mathbb{Z}_q \rtimes_{\xi} \mathbb{Z}_4$
q	-	-	1	-	1
$2q$	-	1	1	1	-
$4q$	1	-	-	-	-

Tabla 4.17: Enumeración de brazas de tipo cíclico de orden $4q$ con $q = 1 \pmod 4$.

4.7.2. Brazas de tipo $\mathbb{Z}_2^2 \times \mathbb{Z}_q$

En estas sección A denotará al grupo $\mathbb{Z}_2^2 \times \mathbb{Z}_q$. Como en la subsección 4.6.2 consideramos el subgrupo de $\mathrm{Aut}\, A \cong GL_2(2) \times \mathbb{Z}_q^{\times}$ que contiene a los elementos de orden a lo sumo 4, que está generado por C y ξ. Este subgrupo es isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_4$ y tiene tres subgrupos de orden 4.

Si G es un subgrupo regular con $|\pi_2(G)| = 2$ entonces se puede aplicar el lema 4.6.4.

Lema 4.7.2. *La única braza de orden* $4q$ *con* $|\ker\lambda| = q$ *es* $(B, +, \circ)$ *donde*

$$\begin{pmatrix} n \\ m \\ l \end{pmatrix} + \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} n+x \\ m+y \\ l+z \end{pmatrix}, \qquad \begin{pmatrix} n \\ m \\ l \end{pmatrix} \circ \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} n + \xi^{2m+l}x \\ m+y+lz \\ l+z \end{pmatrix}$$

para todos $0 \leq n, x \leq q-1$ *y* $0 \leq m, l, y, z \leq 1$. *En particular,* $(B, \circ) \cong \mathbb{Z}_q \rtimes_{\xi} \mathbb{Z}_4$.

Demostración. Si G es un subgrupo regular de $\mathrm{Hol}(A)$ con $|\pi_2(G)| = 4$ entonces el núcleo está generado por ϵ. Si $\pi_2(G) = \langle C, \xi^2 \rangle$, entonces aplicamos el mismo argumento del lema 4.6.3 para llegar a una contradicción. Si $\pi_2(G) = \langle \xi \rangle$ entonces G tiene la siguiente presentación estándar

$$G = \langle \epsilon,\ \sigma^a \tau^b \xi \rangle.$$

Entonces $(\sigma^a \tau^b \xi)^2 = \xi^2 \in G$ y por lo tanto G no es regular. Si $\pi_2(G) = \langle C\xi \rangle$ entonces una presentación estándar de G es

$$G = \langle \epsilon,\ \sigma^a \tau^b C\xi \rangle \cong \mathbb{Z}_q \rtimes_\xi \mathbb{Z}_4.$$

Si $b = 0$ entonces $(\sigma^a C\xi)^2 = \xi^2 \in G$ y luego G no es regular. Entonces $b = 1$ y salvo conjugación por C podemos suponer que $a = 0$. El grupo G es regular. Por lo tanto, en la braza asociada B tenemos $\tau \circ \tau = \tau C(\tau) = \sigma$ y entonces $\lambda_\sigma = \lambda_\tau^2 = \xi^2$. Luego

$$\lambda_{\epsilon^n \sigma^m \tau^l} = \lambda_{\epsilon^n \circ \sigma^m \circ \tau^l} = \lambda_\sigma^m \lambda_\tau^l$$

pues $l = 0, 1$ y se sigue la fórmula. □

La siguiente tabla resume las brazas obtenidas en esta subsección.

$\ker \lambda$	$\mathbb{Z}_{4q}$	$\mathbb{Z}_2^2 \times \mathbb{Z}_q$	$\mathbb{Z}_2 \times (\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_2)$	$\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_4$	$\mathbb{Z}_q \rtimes_\xi \mathbb{Z}_4$
q	-	-	-	-	1
$2q$	1	-	1	1	-
$4q$	-	1	-	-	-

Tabla 4.18: Enumeración de brazas de tipo $\mathbb{Z}_2^2 \times \mathbb{Z}_q$ de orden $4q$ con $q = 1 \pmod 4$.

4.8. Brazas de orden p^2q con p, q aritméticamente independientes

Sean p, q dos números primos. Si no se cumple ninguna de las siguientes congruencias:

$$p = 1 \pmod q, \quad p = -1 \pmod q, \quad q = 1 \pmod p,$$

decimos que p y q son *aritméticamente independientes*. En tal caso, los únicos grupos de orden p^2q son los abelianos: $\mathbb{Z}_{p^2q}$ y $\mathbb{Z}_p^2 \times \mathbb{Z}_q$, [14, Proposition 21.17]. En ambos casos, el orden del núcleo de λ de cualquier braza no trivial es pq. Aplicando los teoremas 4.2.2 y 4.2.6 tenemos la siguiente tabla:

$+\backslash\circ$	$\mathbb{Z}_{p^2q}$	$\mathbb{Z}_p^2 \times \mathbb{Z}_q$
$\mathbb{Z}_{p^2q}$	2	-
$\mathbb{Z}_p^2 \times \mathbb{Z}_q$	-	2

Tabla 4.19: Enumeración de brazas de orden p^2q con p y q aritméticamente independientes.

Capítulo 5

Brazas torcidas de orden p^2q Caso no abeliano

Como resumen de este capítulo enumeramos la cantidad de brazas torcidas de acuerdo con su estructura de grupo aditivo. En la tabla incluimos la referencia a la sección correspondiente en la que se trata cada familia de brazas torcidas.

La clasificación de los grupos de orden p^2q se puede encontrar en [14] y sus grupos de automorfismos en [17].

	Grupos	Secciones
$p = 1 \pmod q$	$\mathbb{Z}_{p^2} \rtimes_t \mathbb{Z}_q$	5.1.1
	$\mathcal{G}_k$	5.1.2, 5.1.3, 5.1.4, 5.1.5
$p = -1 \pmod q$	$\mathcal{G}_F$	5.2
$q = 1 \pmod p$, $q \neq 1 \pmod{p^2}$	$\mathbb{Z}_q \rtimes_r \mathbb{Z}_{p^2}$	5.3.1
	$\mathbb{Z}_p \times (\mathbb{Z}_q \rtimes_r \mathbb{Z}_p)$	5.3.2
$q = 1 \pmod{p^2}$	$\mathbb{Z}_q \rtimes_{h^p} \mathbb{Z}_{p^2}$	5.4.1
	$\mathbb{Z}_p \times (\mathbb{Z}_q \rtimes_{h^p} \mathbb{Z}_p)$	5.4.2
	$\mathbb{Z}_q \rtimes_h \mathbb{Z}_{p^2}$	5.4.3

En cada sección recopilaremos la cantidad de brazas torcidas dando más detalles de cada una.

Las brazas torcidas de tipo no abeliano de orden $2p^2$ fueron enumeradas por Crespo por lo cual no incluimos las tablas correspondientes a este caso y referimos al lector a [27, Section 5]. Si $q = 1 \pmod p$ y $q \neq 1 \pmod{p^2}$ hay 2 grupos no abelianos siempre y cuando $p^2q \neq 12$. Si $p^2q = 12$ hay 3 grupos. Como mencionamos anteriormente, las brazas torcidas de orden 12 están incluidas en la librería *YangBaxter* de GAP, [69], por lo que omitiremos este caso especial.

En [41, Table 5.3] se puede encontrar la cantidad de brazas torcidas de orden $n \leq 120$ con algunas excepciones. Gracias a una mejora en el algoritmo para calcular brazas torcidas, en [13] se pueden consultar varias tablas que recolectan la cantidad de brazas torcidas de orden $n \leq 868$ con algunas excepciones. De todas formas,

ninguna de esas excepciones es de la forma p^2q para primos distintos p, q. Toda esta información se encuentra disponible en [69] y fue de gran valor a la hora de enumerar las brazas torcidas que nos atañen en este y el anterior capítulo. Todos los resultados aquí presentados coinciden con las tablas anteriormente mencionadas.

5.1. Brazas torcidas de orden p^2q con $p = 1 \pmod q$

Sean p, q números primos impares tales que $p = 1 \pmod q$. Recordemos que estamos omitiendo el caso $q = 2$ pues ya fue cubierto por Crespo en [27]. Como fijamos anteriormente, denotamos por g a un elemento fijo de orden q en $\mathbb{Z}_p^\times$ y por t a un elemento fijo de orden q en $\mathbb{Z}_{p^2}^\times$. Los grupos no abelianos de orden p^2q son:

(i) $\mathbb{Z}_{p^2} \rtimes_t \mathbb{Z}_q = \langle \sigma, \tau \mid \sigma^{p^2} = \tau^q = 1,\ \tau\sigma\tau^{-1} = \sigma^t \rangle$.

(ii) $\mathcal{G}_k = \langle \sigma, \tau, \epsilon \,|\, \sigma^p = \tau^p = \epsilon^q = 1,\ \epsilon\sigma\epsilon^{-1} = \sigma^g,\ \epsilon\tau\epsilon^{-1} = \tau^{g^k} \rangle \cong \mathbb{Z}_p^2 \rtimes_{\mathcal{D}_{1,k}} \mathbb{Z}_q$, para cada $k \in \mathfrak{B}$.

Las tablas 5.1 y 5.2 resumen la enumeración de brazas torcidas de acuerdo a la clase de isomorfismo de las estructuras aditiva y multiplicativa teniendo en cuenta que los grupos $\mathcal{G}_k$ y $\mathcal{G}_{k^{-1}}$ son isomorofos si $k \neq 0$.

En particular, si $q = 3$ tenemos $\mathfrak{B} = \{0, 1, -1\}$ y $2^{-1} = 2 = -1$ en $\mathbb{Z}_3^\times$. La enumeración de brazas torcidas sufre una pequeña modificación debido a este hecho por lo cual utilizamos una tabla diferente para el caso de orden $3p^2$.

$+\backslash\circ$	$\mathbb{Z}_{p^2q}$	$\mathbb{Z}_{p^2} \rtimes_t \mathbb{Z}_q$	$\mathbb{Z}_p^2 \times \mathbb{Z}_q$	$\mathcal{G}_s,\ s \neq 0, \pm 1, 2$	$\mathcal{G}_0$	$\mathcal{G}_{-1}$	$\mathcal{G}_1$	$\mathcal{G}_2$
$\mathbb{Z}_{p^2} \rtimes_t \mathbb{Z}_q$	4	$2(q-1)$	-	-	-	-	-	-
$\mathcal{G}_k,\ k \neq 0, \pm 1$	-	-	4	$8(q+1)$	$8(q+1)$	$4(q+1)$	$4(q-1)$	$8(q+1)$
$\mathcal{G}_0$	-	-	2	$4q$	$4q$	$2q$	$2(q-1)$	$4q$
$\mathcal{G}_{-1}$	-	-	3	$4q+p+2$	$4q+p+2$	$3q+p-1$	$2(q-1)$	$4q+p+2$
$\mathcal{G}_1$	-	-	5	$3(q+2)$	$4(q+1)$	$2(q+1)$	$3q-1$	$6q$

Tabla 5.1: Enumeración de brazas torcidas de orden p^2q según la clase de isomorfismo de las estructuras aditiva y multiplicativa para el caso $p = 1 \pmod q$ y $q > 3$.

$+\backslash\circ$	$\mathbb{Z}_{3p^2}$	$\mathbb{Z}_{p^2} \rtimes_t \mathbb{Z}_3$	$\mathbb{Z}_p^2 \times \mathbb{Z}_3$	$\mathcal{G}_0$	$\mathcal{G}_{-1}$	$\mathcal{G}_1$
$\mathbb{Z}_{p^2} \rtimes_t \mathbb{Z}_3$	4	4	-	-	-	-
$\mathcal{G}_0$	-	-	2	12	6	4
$\mathcal{G}_{-1}$	-	-	3	$p+14$	$p+8$	4
$\mathcal{G}_1$	-	-	5	16	10	8

Tabla 5.2: Enumeración de brazas torcidas de orden $3p^2$ según la clase de isomorfismo de las estructuras aditiva y multiplicativa donde $p = 1 \pmod 3$.

5.1.1. Brazas torcidas de tipo $\mathbb{Z}_{p^2} \rtimes_t \mathbb{Z}_q$

En esta sección denotamos por A al grupo $\mathbb{Z}_{p^2} \rtimes_t \mathbb{Z}_q$. De acuerdo con la descripción del grupo de automorfismos de los grupos de orden p^2q que podemos encontrar en [17, Theorem 3.4], tenemos que

$$\phi : \mathrm{Hol}(\mathbb{Z}_{p^2}) = \mathbb{Z}_{p^2} \rtimes \mathbb{Z}_{p^2}^{\times} \longrightarrow \mathrm{Aut}\, A, \quad (i,j) \mapsto \varphi_{i,j} = \begin{cases} \tau \mapsto \sigma^i \tau, \\ \sigma \mapsto \sigma^j \end{cases}$$

es un isomorfismo de grupos. En particular $|\mathrm{Aut}\, A| = p^3(p-1)$. Luego, si G es un subgrupo regular de $\mathrm{Hol}(A)$ entonces $|\pi_2(G)| \in \{p, q, p^2, pq, p^2q\}$. Veamos que $|\pi_2(G)|$ no puede ser igual a p.

Lema 5.1.1. *Sea G un subgrupo regular de $\mathrm{Hol}(A)$. Entonces $|\pi_2(G)| \neq p$.*

Demostración. Supongamos que G es un subgrupo de orden p^2q de $\mathrm{Hol}(A)$ y que $|\pi_2(G)| = p$. Salvo conjugación podemos elegir los generadores de $\ker \pi_2|_G$ para que sean τ y σ^p. Por lo tanto la presentación estándar de G es

$$G = \langle \tau, \sigma^p, \sigma^a \alpha \rangle$$

donde $\alpha \in \mathrm{Aut}\, A$ es un automorfismo de orden p que satisface que $\alpha(\tau) = \sigma^{pb}\tau$ para cierto $0 \leq b \leq p-1$. Por la condición (K) tenemos que

$$\sigma^a \alpha \tau \alpha^{-1} \sigma^{-a} = \sigma^{a(1-t)+pb}\tau \in \langle \sigma^p, \tau \rangle.$$

Entonces $a = 0 \pmod p$, es decir $a = a'p$.

Luego, $(\sigma^p)^{-a'}\sigma^{a'p}\alpha = \alpha \in G \cap (\{1\} \times \mathrm{Aut}\, A)$ y entonces G no es regular por el lema 4.1.3. □

Lema 5.1.2. *Existe una única clase de conjugación de subgrupos regulares G de $\mathrm{Hol}(A)$ con $|\pi_2(G)| = pq$. Un representante es*

$$H = \langle \sigma^p,\ \sigma\varphi_{0,p+1},\ \tau^{-1}\varphi_{0,t} \rangle \cong \mathbb{Z}_{p^2q}.$$

Demostración. De acuerdo con el lema 4.1.4(2) tenemos que $\langle \sigma^p, \tau \rangle \subseteq \pi_1(H)$ y claramente $\sigma \in \pi_1(H)$. Luego $|\pi_1(H)| > pq$ y entonces $|\pi_1(H)| = |H| = p^2q$. Por el lema 4.1.3, H es regular.

Sea G un subgrupo regular de $\mathrm{Hol}(A)$ que cumple que $|\pi_2(G)| = pq$. Entonces $K = \ker \pi_2|_G = \langle \sigma^p \rangle$. Salvo conjugación, los subgrupos de orden pq de $\mathrm{Aut}\, A$ son $\langle \varphi_{p,1},\ \varphi_{0,t} \rangle$ y $\langle \varphi_{0,t},\ \varphi_{0,p+1} \rangle$.

En el primer caso, tenemos

$$G = \langle \sigma^p,\ \sigma^a\tau^b\varphi_{p,1},\ \sigma^c\tau^d\varphi_{0,t} \rangle.$$

Debemos verificar las condiciones (R). Los generadores de $\pi_2(G)$ satisfacen las relaciones $(\varphi_{p,1})^p = 1$ y $\varphi_{0,t}\varphi_{p,1}\varphi_{0,t}^{-1} = \varphi_{p,1}^t$. Por lo tanto, tenemos

$$(\sigma^a\tau^b\varphi_{p,1})^p K = \sigma^{a\sum_{j=0}^{p-1} t^{bj}} \tau^{bp} K \overset{(R)}{=} K$$

y entonces $b = 0$. En consecuencia $d \neq 0$ porque de otra manera, por el lema 4.1.4(1) tendríamos que $\pi_1(G) \subseteq \langle\sigma\rangle$. Más aún

$$(\sigma^c\tau^d\varphi_{0,t})\sigma^a\varphi_{p,1}\left(\sigma^c\tau^d\varphi_{0,t}\right)^{-1}K = \sigma^{t^{d+1}a}\varphi_{p,1}^tK \overset{(R)}{=} (\sigma^a\varphi_{p,1})^tK = \sigma^{ta}\varphi_{p,1}^tK$$

y entonces $a = pa'$. Consecuentemente, $\sigma^{-a'p}\sigma^{a'p}\varphi_{p,1} = \varphi_{p,1} \in G$ y entonces G no es regular, lo cual es una contradicción.

Sea $\pi_2(G) = \langle\varphi_{0,t},\ \varphi_{0,p+1}\rangle$. Entonces

$$G = \langle\sigma^p,\ \sigma^a\tau^b\varphi_{0,p+1},\ \sigma^c\tau^d\varphi_{0,t}\rangle.$$

Los generadores de $\pi_2(G)$ satisfacen las relaciones

$$\varphi_{0,t}^q = \ \varphi_{0,p+1}^p = [\varphi_{0,t}, \varphi_{0,p+1}] = 1.$$

Por las condiciones (R) tenemos que $\sigma^a\tau^b\varphi_{0,p+1}$ y $\sigma^c\tau^d\varphi_{0,t}$ satisfacen las mismas relaciones módulo K. Por consiguiente, como

$$\begin{aligned}(\sigma^a\tau^b\varphi_{0,p+1})^pK &= \sigma^{a\sum_{j=0}^{p-1}t^{bj}}\tau^{bp}K \overset{(R)}{=} K,\\ (\sigma^a\varphi_{0,p+1})\sigma^c\tau^d\varphi_{0,t}K &= \sigma^{a+c}\tau^d\varphi_{0,p+1}\varphi_{0,t}K \overset{(R)}{=} (\sigma^c\tau^d\varphi_{0,t})\sigma^a\varphi_{0,p+1}K\\ &= \sigma^{t^{d+1}a+c}\tau^d\varphi_{0,p+1}\varphi_{0,t}K\end{aligned}$$

entonces $b = 0$ y $d = -1$. Finalmente,

$$(\sigma^c\tau^{-1}\varphi_{0,t})^qK = \sigma^{qc}K \overset{(R)}{=} K$$

y entonces $c = 0 \pmod p$.

Si $a = 0 \pmod p$, por el lema 4.1.4(2), tenemos $\pi_1(G) \subseteq \langle\sigma^p, \tau\rangle$ y entonces $a \neq 0 \pmod p$. Luego, G es un conjugado de H por $\varphi_{0,a^{-1}}$. □

Lema 5.1.3. *Un conjunto de representantes de subgrupos regulares G de* $\mathrm{Hol}(A)$ *con $|\pi_2(G)| = p^2$ está dado por*

$$G_s = \langle\tau,\ \sigma^{\frac{1}{t-1}}\varphi_{1,(p+1)^s}\rangle \cong \mathbb{Z}_{p^2q}$$

para $s = 0, 1$.

Demostración. Los grupos G_0 y G_1 no son conjudados entre sí puesto que sus imágenes por π_2 no lo son. Aplicando el lema 4.1.3 y el lema 4.1.4 como lo hicimos en el lema 5.1.2, podemos ver que los grupos G_s son regulares. En efecto, $(\sigma^{\frac{1}{t-1}}\varphi_{1,(p+1)^s})^p = \sigma^{\frac{p}{t-1}}\varphi_{p,1}$ y $\varphi_{p,1}(\sigma^{\frac{p}{t-1}}) = \sigma^{\frac{p}{t-1}}$. Por lo tanto, tenemos que $\langle\tau, \sigma^p\rangle \subseteq \pi_1(G_s)$ y $\sigma^{\frac{1}{t-1}} \in \pi_1(G_s)$. Luego $|\pi_1(H)| = p^2q$ y entonces H es regular.

Sea G un subgrupo regular de $\mathrm{Hol}(A)$ con $|\pi_2(G)| = p^2$. Por el lema 4.1.1, el p-subgrupo de Sylow del grupo multiplicativo de la braza torcida asociada a G es cíclico y en consecuencia también lo es $\pi_2(G)$. Los únicos subgrupos cíclicos de orden p^2 de $\mathrm{Aut}\,A$ salvo conjugación son $\langle\varphi_{1,(p+1)^s}\rangle$ para $s = 0, 1$. El orden del núcleo de

π_2 es q y entonces, en ambos casos podemos asumir que $\ker \pi_2|_G$ está generado por τ salvo conjugación por un automorfismo del normalizador de $\pi_2(G)$. En consecuencia

$$G = \langle \tau,\ \sigma^b \varphi_{1,(p+1)^s} \rangle$$

para cierto $b \neq 0$. El grupo G tiene un q-subgrupo de Sylow normal y entonces es abeliano, por lo tanto $b = \frac{1}{t-1}$. □

El grupo

$$\mathfrak{H}_1 = \langle \sigma, \varphi_{1,1} \rangle \tag{5.1}$$

es normal en $\mathrm{Hol}(A)$.

Sea u un generador de $\mathbb{Z}_{p^2}^\times$, entonces $\mathrm{Hol}(A)/\mathfrak{H}_1 = \langle \tau,\ \varphi_{0,u} \rangle \cong \mathbb{Z}_q \times \mathbb{Z}_{p^2}^\times$ y en particular es abeliano.

Lema 5.1.4. *Las brazas torcidas de tipo A con $|\ker \lambda| = p^2$ son $B_s = (A, +, \circ)$ donde $(B_s, +) = \mathbb{Z}_{p^2} \rtimes_t \mathbb{Z}_q$ y $(B_s, \circ) = \mathbb{Z}_{p^2} \rtimes_{t^{\frac{s+1}{s}}} \mathbb{Z}_q$ con $1 \leq s \leq q-1$.*

En particular, B_s es una bi-braza y

$$(B_s, \circ) \cong \begin{cases} \mathbb{Z}_{p^2q}, & \text{si } s = q-1, \\ A, & \text{en otro caso.} \end{cases}$$

Demostración. Consideremos los grupos

$$G_s = \langle \sigma,\ \tau^s \varphi_{0,t} \rangle \cong \begin{cases} \mathbb{Z}_{p^2q}, & \text{si } s = q-1, \\ A, & \text{en otro caso} \end{cases}$$

para $1 \leq s \leq q-1$. El subconjunto $\pi_1(G_s)$ contiene a $\langle \sigma \rangle$ y τ^s y entonces $|\pi_1(G)| > p^2$ y además divide a p^2q. Luego, $\pi_1(G) = A$ y por el lema 4.1.3 tenemos que G_s es regular. Sea $\mathfrak{H}_1$ el grupo definido en (5.1). Si G_s y $G_{s'}$ son conjugados entre sí, entonces sus imágenes en el cociente $\mathrm{Hol}(A)/\mathfrak{H}_1$, que es abeliano, también lo son. Entonces $\langle \tau^s \varphi_{0,t} \rangle = \langle \tau^{s'} \varphi_{0,t} \rangle$ y se sigue que $s = s'$.

Sea G un subgrupo regular de $\mathrm{Hol}(A)$ con $|\pi_2(G)| = q$. El único subgrupo de orden p^2 de A es el único p-subgrupo de Sylow generado por σ y, salvo conjugación, el único subgrupo de orden q de $\mathrm{Aut}\, A$ está generado por $\varphi_{0,t}$. Entonces

$$G = \langle \sigma, \tau^s \varphi_{0,t} \rangle = G_s$$

para cierto $s \neq 0$.

Si B_s es la braza torcida asociada a G_s tenemos que $\langle \sigma \rangle \leq \ker \lambda$ y $\tau \in \mathrm{Fix}(B_s)$. Luego, usando el lema 4.1.2 tenemos que $\lambda_{\sigma^n \tau^m} = \lambda_{\sigma^n \tau^{\frac{sm}{s}}} = \lambda_{\tau^s}^m$ y entonces la estructura multiplicativa de B_s viene dada por la fórmula

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \circ \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} x_1 + t^{\frac{s+1}{s} x_2} y_1 \\ x_2 + y_2 \end{pmatrix}$$

para todos $0 \leq x_1, y_1 \leq p^2 - 1$, $0 \leq x_2, y_2 \leq q-1$.

Luego, $(B_s, +) = \mathbb{Z}_{p^2} \rtimes_t \mathbb{Z}_q$ y $(B_s, \circ) = \mathbb{Z}_{p^2} \rtimes_{t^{\frac{s+1}{s}}} \mathbb{Z}_q$ y de acuerdo con el corolario 3.1.2, B_s es una bi-braza. Para calcular la clase de isomorfismo de $(B_s, \circ)$ notemos que es abeliano si y sólo si $s = q-1$. □

Lema 5.1.5. *Un conjunto de representantes de las clases de conjugación de los subgrupos regulares G de* $\mathrm{Hol}(A)$ *con* $|\pi_2(G)| = p^2q$ *es*

$$G_d = \langle \sigma^{\frac{1}{t-1}}\varphi_{1,1},\ \tau^d\varphi_{0,t}\rangle \cong A$$

donde $1 \leq d \leq q-1$.

Demostración. Por el lema 4.1.4(2), $\langle \sigma, \tau\rangle \subseteq \pi_1(G_d)$ y entonces $\pi_1(G_d) = A$. Por el mismo argumento que usamos en el lema 5.1.4 podemos ver que no son conjugados entre sí.

Sea G un subgrupo regular con $|\pi_2(G)| = p^2q$. Por el lema 4.1.1, el p-subgrupo de Sylow del grupo multiplicativo de la braza torcida asociada a G es cíclico y entonces también lo es el p-subgrupo de Sylow de $\pi_2(G)$. Salvo conjugación podemos asumir que $\pi_2(G)$ es $\langle \varphi_{1,1},\ \varphi_{0,t}\rangle \cong A$, es decir

$$G = \langle \sigma^a\tau^b\varphi_{1,1},\ \sigma^c\tau^d\varphi_{0,t}\rangle.$$

Por las condiciones (R) tenemos

$$(\sigma^a\tau^b\varphi_{1,1})^{p^2} = 1, \tag{5.2}$$

$$(\sigma^c\tau^d\varphi_{0,t})^q = 1, \tag{5.3}$$

$$(\sigma^c\tau^d\varphi_{0,t})\sigma^a\tau^b\varphi_{1,1}(\sigma^c\tau^d\varphi_{0,t})^{-1} = (\sigma^a\tau^b\varphi_{1,1})^t. \tag{5.4}$$

la igualdad (5.2) implica que la misma relación es válida módulo $\mathfrak{H}_1$ y entonces $b = 0$. Si $d = 0$ entonces G no es regular por el lema 4.1.4(1). Por consiguiente $d \neq 0$ y por (5.4) tenemos que $a = \frac{1}{t-1}$ y entonces la presentación estándar de G es

$$G = \langle \sigma^{\frac{1}{t-1}}\varphi_{1,1},\ \sigma^c\tau^d\varphi_{0,t}\rangle.$$

Si $d = -1$ entonces deducimos que $c = 0$ a partir de (5.3). De otra forma, G es un conjugado de G_d por $\varphi_{1,1}^n$ donde $n = \frac{c(t-1)}{1-t^{d+1}}$. □

La siguiente tabla resume el contenido de esta subsección:

$\lvert\ker\lambda\rvert$	$\mathbb{Z}_{p^2q}$	$\mathbb{Z}_{p^2} \rtimes_t \mathbb{Z}_q$
1	-	$q-1$
p	1	-
q	2	-
p^2	1	$q-2$
p^2q	-	1

Tabla 5.3: Enumeración de las brazas torcidas de tipo $\mathbb{Z}_{p^2} \rtimes_t \mathbb{Z}_q$ para $p = 1 \pmod q$.

5.1.2. Brazas torcidas de tipo $\mathcal{G}_k$ para $k \neq 0, \pm 1$

En esta sección asumiremos que $k \in \mathfrak{B} \setminus \{0, 1, -1\}$ y por consiguiente que $q > 3$. Recordemos una presentación del grupo $\mathcal{G}_k$:

$$\mathcal{G}_k = \langle \sigma, \tau, \epsilon \;\big|\; \sigma^p = \tau^p = \epsilon^q = [\sigma, \tau] = 1,\ \epsilon\sigma\epsilon^{-1} = \sigma^g,\ \epsilon\tau\epsilon^{-1} = \tau^{g^k} \rangle \tag{5.5}$$

donde g es un elemento fijo de orden q en $\mathbb{Z}_p^\times$ como antes. Un automorfismo de $\mathcal{G}_k$ está determinado por la imagen de los generadores, es decir por la restricción a $\langle \sigma, \tau \rangle$ dada por una matriz y por la imagen de ϵ. De acuerdo con [17, Subsections 4.1, 4.3], la función

$$\begin{array}{rcl} \phi : \mathbb{Z}_p^2 \rtimes_\rho \left(\mathbb{Z}_p^\times \times \mathbb{Z}_p^\times\right) & \longrightarrow & \operatorname{Aut} \mathcal{G}_k, \\ [(n,m),(a,b)] & \mapsto & h = \begin{cases} h|_{\langle \sigma,\tau \rangle} = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}, \\ \epsilon \mapsto \sigma^n \tau^m \epsilon, \end{cases} \end{array}$$

es un isomorfismo de grupos (la acción ρ se define como $\rho(a,b)(n,m) = (an, bm)$). En particular, $|\operatorname{Aut} \mathcal{G}_k| = p^2(p-1)^2$ y el único p-subgrupo de Sylow de $\operatorname{Aut} \mathcal{G}_k$ está generado por $\alpha_1 = [(1,0),(1,1)]$ y $\alpha_2 = [(0,1),(1,1)]$.

Sea G un subgrupo regular de $\operatorname{Hol}(\mathcal{G}_k)$. Como p^2q divide a $|\operatorname{Aut} G_k|$ debemos tener en cuenta todos los casos posibles para el orden de $\pi_2(G)$.

En $\operatorname{Hol}(\mathcal{G}_k)$ se cumple que

$$(\sigma^a\tau^b\alpha_1)\epsilon(\sigma^a\tau^b\alpha_1)^{-1} = \sigma^{1+(1-g)a}\tau^{(1-g^k)b}\epsilon, \tag{5.6}$$

$$(\sigma^c\tau^d\alpha_2)\epsilon(\sigma^c\tau^d\epsilon\alpha_2)^{-1} = \sigma^{(1-g)c}\tau^{1+(1-g^k)d}\epsilon, \tag{5.7}$$

para todos $0 \leq a, b, c, d \leq p-1$.

Lema 5.1.6. *Un conjunto de representantes de clases de conjugación de subgrupos regulares G de* $\operatorname{Hol}(\mathcal{G}_k)$ *con* $|\pi_2(G)| = p$ *está dado por*

$$H_i = \langle \epsilon, \tau, \sigma^{\frac{1}{g-1}}\alpha_1\alpha_2^i \rangle \cong \mathcal{G}_0, \quad K_i = \langle \epsilon, \sigma, \tau^{\frac{1}{g^k-1}}\alpha_1^i\alpha_2 \rangle \cong \mathcal{G}_0,$$

con $i = 0, 1$.

Demostración. Salvo conjugación, los subgrupos de orden p de $\operatorname{Aut} \mathcal{G}_k$ son $\langle \alpha_1 \rangle, \langle \alpha_2 \rangle$ y $\langle \alpha_1\alpha_2 \rangle$. Los grupos del enunciado no son conjugados entre sí pues o bien sus imágenes o bien sus núcleos con respecto a π_2 no lo son. Cualquiera de ellos tiene la forma

$$G = \langle \epsilon, u, v\theta \rangle$$

con $\theta(v) = v$ y $\mathcal{G}_k = \langle \epsilon, u, v \rangle$. Por el lema 4.1.4(2), $\pi_1(G) = \mathcal{G}_k$, es decir G es regular.

Sea G un subgrupo regular de $\operatorname{Hol}(\mathcal{G}_k)$ con $|\pi_2(G)| = p$. El núcleo de π_2 tiene orden pq y entonces contiene un elemento de orden q que será de la forma $u\epsilon$ donde $u \in \langle \sigma, \tau \rangle$. El subgrupo $L = \langle \alpha_1, \alpha_2 \rangle$ normaliza a $\pi_2(G)$ por lo cual podemos conjugar

a G por un elemento conveniente de L y por (5.6) y (5.7) podemos suponer que $u = 0$. Luego, el núcleo tiene la forma $\langle \epsilon,\ v\rangle$ para cierto $v \in \langle \sigma, \tau\rangle$. El p-subgrupo de Sylow de $\ker \pi_2$ es normal y entonces $v = \sigma$ o τ. Por lo tanto, el grupo G tiene la forma

$$G = \langle \epsilon, v, w\theta\rangle$$

donde $\theta \in \{\alpha_1, \alpha_2, \alpha_1\alpha_2\}$ y, o bien $v = \sigma$ y $1 \neq w \in \langle\tau\rangle$ o bien $v = \tau$ y $1 \neq w \in \langle\sigma\rangle$. Por la condición (K) debemos verificar que

$$w\theta\epsilon\theta^{-1}w^{-1} = w\theta(\epsilon)w^{-1} \in \ker \pi_2|_G.$$

Por (5.6) y (5.7) se sigue que G es H_i o K_i para algún $i = 0, 1$. □

Lema 5.1.7. *La única braza torcida de tipo $\mathcal{G}_k$ con $|\ker\lambda| = q$ es $(B, +, \circ)$ donde $(B, +) = \mathbb{Z}_p^2 \rtimes_{\mathcal{D}_{1,k}} \mathbb{Z}_q$ y*

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \circ \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} x_1 g^{y_3} + y_1 g^{x_3} \\ x_2 g^{ky_3} + y_2 g^{kx_3} \\ x_3 + y_3 \end{pmatrix}.$$

para todos $0 \leq x_1, x_2, y_1, y_2 \leq p-1$ y $0 \leq x_3, y_3 \leq q-1$.

En particular, $(B, \circ) \cong \mathbb{Z}_p^2 \times \mathbb{Z}_q$.

Demostración. De acuerdo con (5.6) y (5.7), el subgrupo

$$H = \langle \epsilon,\ \sigma^{\frac{1}{g-1}}\alpha_1,\ \tau^{\frac{1}{g^k-1}}\alpha_2\rangle$$

es isomorfo a $\mathbb{Z}_p^2 \times \mathbb{Z}_q$ y $|\pi_2(G)| = p^2$. Por el lema 4.1.4(2), $\pi_1(H) = \langle \epsilon, \sigma, \tau\rangle$ y entonces H es regular.

Sea G un subgrupo regular con $|\pi_2(G)| = p^2$. Entonces la imagen de π_2 es el único p-subgrupo de Sylow de $\operatorname{Aut}\mathcal{G}_k$. El núcleo es un subgrupo de orden q de G y, por (5.6) y (5.7), podemos suponer que está generado por ϵ. El grupo G tiene la presentación estándar

$$G = \langle \epsilon,\ \sigma^a\tau^b\alpha_1,\ \sigma^c\tau^d\alpha_2\rangle$$

y es abeliano pues tiene un q-subgrupo de Sylow normal. Por (5.6) y (5.7) nuevamente, tenemos que $b = c = 0$, $a = \frac{1}{g-1}$ y $d = \frac{1}{g^k-1}$, es decir $G = H$.

Sea B la braza torcida asociada a H. Como $\epsilon \in \ker\lambda$ y $\sigma, \tau \in \operatorname{Fix}(B)$, por el lema 4.1.2 podemos hallar la fórmula del enunciado para la operación $\circ$ de B. □

El subgrupo

$$\mathfrak{H}_2 = \langle \sigma,\ \tau,\ \alpha_1,\ \alpha_2\rangle \cong \mathbb{Z}_p^4 \tag{5.8}$$

es normal en $\operatorname{Hol}(\mathcal{G}_k)$. Sea μ un generador de $\mathbb{Z}_p^\times$, entonces

$$\operatorname{Hol}(\mathcal{G}_k)/\mathfrak{H}_2 = \langle \epsilon, [(0,0),(1,\mu)], [(0,0),(\mu,1)]\rangle \cong \mathbb{Z}_q \times \mathbb{Z}_p^\times \times \mathbb{Z}_p^\times.$$

En particular, es abeliano.

En el grupo $\mathrm{Hol}(\mathcal{G}_k)$ se cumple que

$$\alpha_1^n\alpha_2^m u\epsilon^d\theta\alpha_2^{-m}\alpha_1^{-n} = u\sigma^{xn\frac{g^d-1}{g-1}}\alpha_1^{(1-x)n}\tau^{ym\frac{g^{kd}-1}{g^k-1}}\alpha_2^{(1-y)m}\epsilon^d\theta, \qquad (F_k)$$

para $u \in \langle\sigma,\tau\rangle$ y $\theta = [(0,0),(x,y)]$.

Fijemos los elementos $\beta_s = [(0,0),(g,g^s)]$ y $\widetilde{\beta} = [(0,0),(1,g)]$ para $0 \le s \le q-1$.

Proposición 5.1.8. *Las brazas torcidas de tipo $\mathcal{G}_k$ con $|\ker\lambda| = p^2$ son $(B_{a,b},+,\circ)$ donde $(B_{a,b},+) = \mathbb{Z}_p^2 \rtimes_{\mathcal{D}_{1,k}} \mathbb{Z}_q$ y*

$$(B_{a,b},\circ) = \mathbb{Z}_p^2 \rtimes_{\mathcal{D}_{a+1,b+k}} \mathbb{Z}_q \cong \begin{cases} \mathbb{Z}_p^2\times\mathbb{Z}_q, & \text{si } a = q-1,\ b = -k \pmod q,\\ \mathcal{G}_0, & \text{si } a = q-1,\ b \neq -k \pmod q,\\ \mathcal{G}_{\frac{b+k}{a+1}}, & \text{en otro caso,}\end{cases}$$

para todos $0 \le a,b \le q-1$ y $(a,b) \neq (0,0)$. En particular, hay q^2-1 brazas torcidas de esta forma y todas ellas son bi-brazas.

Demostración. Los subgrupos

$$G_{a,b} = \langle\sigma,\ \tau,\ \epsilon\beta_0^a\widetilde{\beta}^b\rangle$$

son regulares. Si $G_{a,b}$ y $G_{c,d}$ son conjugados entonces también lo son sus proyecciones al cociente $\mathrm{Hol}(\mathcal{G}_k)/\mathfrak{H}_2$ que es abeliano. Entonces $\langle\epsilon\beta_0^a\widetilde{\beta}^b\rangle = \langle\epsilon\beta_0^c\widetilde{\beta}^d\rangle$ y se sigue que $(a,b) = (c,d)$.

Sea G un subgrupo regular de $\mathrm{Hol}(\mathcal{G}_k)$ tal que $|\pi_2(G)| = q$. Entonces el núcleo de π_2 es el único p-subgrupo de Sylow de $\mathcal{G}_k$. Los elementos de orden q de $\mathrm{Aut}\,\mathcal{G}_k$ son de la forma $\alpha_1^s\alpha_2^t\beta_0^a\widetilde{\beta}^b$ donde $s = 0$ (resp. $t = 0$) siempre que $a = 0$ (resp. $b = 0$). Por (F_k) para $u = 1$ y $d = 0$, salvo conjugación por un elemento de $\langle\alpha_1,\alpha_2\rangle$, podemos suponer que $\pi_2(G)$ está generado por $\beta_0^a\widetilde{\beta}^b$ donde $(a,b) \neq (0,0)$. Luego,

$$G = \langle\sigma,\ \tau,\ \epsilon^n\beta_0^a\widetilde{\beta}^b\rangle$$

y entonces $n \neq 0$ pues G es regular. Usando que $(\epsilon^n\beta_0^a\widetilde{\beta}^b)^{n^{-1}} = \epsilon\beta_0^{an^{-1}}\widetilde{\beta}^{bn^{-1}}$ podemos concluir que $G = G_{an^{-1},bn^{-1}}$.

Sea $B_{a,b}$ la braza torcida asociada al subgrupo regular $G_{a,b}$. Notemos que se cumple que $\epsilon \in \mathrm{Fix}(B_{a,b})$ y $\sigma,\tau \in \ker\lambda$. Por lo tanto, pordemos aplicar el lema 4.1.2 y se sigue que

$$\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix} \circ \begin{pmatrix}y_1\\y_2\\y_3\end{pmatrix} = \begin{pmatrix}x_1 + g^{(a+1)x_3}y_1\\ x_2 + g^{(b+k)x_3}y_2\\ x_3+y_3\end{pmatrix} \qquad (5.9)$$

para todos $0 \le x_1,x_2,y_1,y_2 \le p-1$, $0 \le x_3,y_3 \le q-1$.

Por lo tanto, $(B_{a,b},+) = \mathbb{Z}_p^2 \rtimes_{\mathcal{D}_{1,k}} \mathbb{Z}_q$, $(B_{a,b},\circ) = \mathbb{Z}_p^2 \rtimes_{\mathcal{D}_{a+1,b+k}} \mathbb{Z}_q$ y las imágenes de las dos acciones conmutan. Por la proposición 3.1.1 es una bi-braza. □

Para calcular los subgrupos regulares de $\mathrm{Hol}(\mathcal{G}_k)$ cuya imagen por π_2 tienen orden pq o p^2q debemos calcular las clases de conjugación de subgrupos de orden pq y p^2q de $\mathrm{Aut}\,\mathcal{G}_k$.

Lema 5.1.9. *Un conjunto de representantes de clases de conjugación de subgrupos de* $\mathrm{Aut}\,\mathcal{G}_k$ *de orden* pq *y orden* p^2q *está dado por la siguiente tabla*

Orden	G	*Parámetros*	*Clase*
pq	$\mathcal{H}_{1,s} = \langle \alpha_1, \beta_s \rangle$	$0 \le s \le q-1$	$\mathbb{Z}_p \rtimes_t \mathbb{Z}_q$
	$\mathcal{H}_{2,s} = \langle \alpha_2, \beta_s \rangle$	$0 \le s \le q-1$	$\mathbb{Z}_{pq}$, *si* $s = 0$,
			$\mathbb{Z}_p \rtimes_t \mathbb{Z}_q$, *en otro caso.*
	$\mathcal{K}_i = \langle \alpha_i, \widetilde{\beta} \rangle$	$i = 1, 2$	$\mathbb{Z}_{pq}$, *si* $i = 1$,
			$\mathbb{Z}_p \rtimes_t \mathbb{Z}_q$, *si* $i = 2$.
	$\mathcal{W} = \langle \alpha_1\alpha_2, \beta_1 \rangle$	-	$\mathbb{Z}_p \rtimes_t \mathbb{Z}_q$
p^2q	$\mathcal{T}_s = \langle \alpha_1, \alpha_2, \beta_s \rangle$	$0 \le s \le q-1$	$\mathcal{G}_s$
	$\mathcal{U} = \langle \alpha_1, \alpha_2, \widetilde{\beta} \rangle$	-	$\mathcal{G}_0$

Demostración. Sea G un subgrupo de orden pq de $\mathrm{Aut}\,\mathcal{G}_k$. Entonces G está generado por un elemento de orden p y un elemento de orden q. Los elementos de orden p pertenecen al subgrupo generado por α_1 y α_2 y, salvo conjugación, hay tres elementos de orden p, digamos $\alpha_1, \alpha_2, \alpha_1\alpha_2$. Los elementos de orden q se pueden elegir de la forma $\alpha_1^n\alpha_2^m\beta_s$ para $s \neq 0$, $\alpha_1^n\beta_0$ o $\alpha_2^m\widetilde{\beta}$.

Si el p-subgrupo de Sylow de G está generado por α_i, $i = 1, 2$, usando que

$$\begin{aligned} [(a,b),(x,y)]\alpha_1^n\alpha_2^m\beta_s[(a,b),(x,y)]^{-1} &= \alpha_1^{xn+(1-g)a}\alpha_2^{ym+(1-g^s)b}\beta_s, \\ [(a,b),(x,y)]\alpha_2^m\widetilde{\beta}[(a,b),(x,y)]^{-1} &= \alpha_2^{ym+(1-g)b}\widetilde{\beta}, \end{aligned} \tag{5.10}$$

tenemos que G es un conjugado de $\mathcal{H}_{i,s}$ o de $\mathcal{K}_i$. Si el p-subgrupo de Sylow de G está generado por $\alpha_1\alpha_2$ entonces necesariamente el elemento de orden q es de la forma $\alpha_1^n\alpha_2^m\beta_1$, pues el p-subgrupo de Sylow debe ser normal. En este caso, entonces $G = \langle \alpha_1\alpha_2,\ \alpha_1^n\alpha_2^m\beta_1 \rangle = \langle \alpha_1\alpha_2,\ \alpha_1^{n-m}\beta_1 \rangle$ y de acuerdo con (5.10), G es un conjugado de $\mathcal{W}$ por una potencia adecuada de α_1.

Si G es un subgrupo de orden p^2q entonces G está generado por α_1, α_2 y un elemento de orden q que podemos pensar que es β_s para algún $0 \le s \le q-1$ o bien $\widetilde{\beta}$. Tales grupos no son conjugados puesto que sus restricciones a $\langle \sigma, \tau \rangle$ no lo son. □

En lo que sigue utilizaremos la misma notación del lema 5.1.9 y la siguiente fórmula:

$$(\sigma^a\tau^b\epsilon^c\theta)^n = \sigma^{a\sum_{i=0}^{n-1} g^{i(c+x)}}\tau^{a\sum_{i=0}^{n-1} g^{i(ck+y)}}\epsilon^{nc}\theta^n \tag{P_k}$$

donde $\theta = [(0,0),(g^x,g^y)]$.

Lema 5.1.10. *Un conjunto de representantes de las clases de equivalencia de subgrupos regulares* G *de* $\mathrm{Hol}(\mathcal{G}_k)$ *con* $|\pi_2(G)| = pq$ *está dado por la tabla 5.4 de la página 81.*

$\pi_2(G)$	Subgrupos	Parámetros	Clase de isomorfismo	#
$\mathcal{H}_{1,s}$	$\widetilde{H}_{1,s,d} = \langle \tau, \sigma^{\frac{1}{g-1}}\alpha_1, \epsilon^d\beta_s\rangle$	$0 \leq s \leq q-1$, $1 \leq d \leq q-1$	$\mathcal{G}_{dk+s}$	$q(q-1)$
	$\widehat{H}_{1,s} = \langle \sigma, \tau\alpha_1, \epsilon^{\frac{1-s}{k}}\beta_s\rangle$	$2 \leq s \leq q$	$\mathcal{G}_{\frac{k-s+1}{k}}$	$q-1$
	$\overline{H}_{1,s} = \langle \sigma\tau, \sigma^{\frac{1}{g-1}}\alpha_1, \epsilon^{\frac{s-1}{1-k}}\beta_s\rangle$	$2 \leq s \leq q$	$\mathcal{G}_{\frac{s-k}{1-k}}$	$q-1$
$\mathcal{H}_{2,s}$	$\widetilde{H}_{2,s,d} = \langle \sigma, \tau^{\frac{1}{g^k-1}}\alpha_2, \epsilon^d\beta_s\rangle$	$0 \leq s \leq q-1$, $1 \leq d \leq q-1$	$\mathbb{Z}_p^2 \times \mathbb{Z}_q$, si $s = 0, d = -1$, $\mathcal{G}_0$, si $s \neq 0$, $d = -1$, $\mathcal{G}_{\frac{s}{d+1}}$, en otro caso.	$q(q-1)$
	$\widehat{H}_{2,s} = \langle \tau, \sigma\alpha_2, \epsilon^{s-1}\beta_s\rangle$	$2 \leq s \leq q$	$\mathcal{G}_0$, si $s = 0$, $\mathcal{G}_{\frac{s(k+1)-k}{s}}$, en otro caso.	$q-1$
	$\overline{H}_{2,s} = \langle \sigma\tau, \tau^{\frac{1}{g^k-1}}\alpha_2, \epsilon^{\frac{s-1}{1-k}}\beta_s\rangle$	$2 \leq s \leq q$	$\mathcal{G}_0$ si $s = 0$, $\mathcal{G}_{\frac{s-k}{s(1-k)}}$, en otro caso.	$q-1$
$\mathcal{K}_1$	$\widetilde{K}_{1,d} = \langle \tau, \sigma^{\frac{1}{g-1}}\alpha_1, \epsilon^d\widetilde{\beta}\rangle$	$1 \leq d \leq q-1$	$\mathbb{Z}_p^2 \times \mathbb{Z}_q$ si $d = -k^{-1}$, $\mathcal{G}_0$, en otro caso.	$q-1$
	$\widehat{K}_1 = \langle \sigma, \tau\alpha_1, \epsilon^{-k^{-1}}\widetilde{\beta}\rangle$	-	$\mathcal{G}_0$	1
	$\overline{K}_1 = \langle \sigma\tau, \sigma^{\frac{1}{g-1}}\alpha_1, \epsilon^{\frac{1}{1-k}}\widetilde{\beta}\rangle$	-	$\mathcal{G}_0$	1
$\mathcal{K}_2$	$\widetilde{K}_{2,d} = \langle \sigma, \tau^{\frac{1}{g^k-1}}\alpha_2, \epsilon^d\widetilde{\beta}\rangle$	$1 \leq d \leq q-1$	$\mathcal{G}_d$	$q-1$
	$\widehat{K}_2 = \langle \tau, \sigma\alpha_2, \epsilon\widetilde{\beta}\rangle$	-	$\mathcal{G}_{k+1}$	1
	$\overline{K}_2 = \langle \sigma\tau, \tau^{\frac{1}{g^k-1}}\alpha_2, \epsilon^{\frac{1}{1-k}}\widetilde{\beta}\rangle$	-	$\mathcal{G}_{\frac{1}{1-k}}$	1
$\mathcal{W}$	$\widetilde{W}_d = \langle \sigma, \tau^{\frac{1}{g^k-1}}\alpha_1\alpha_2, \epsilon^d\beta_1\rangle$	$1 \leq d \leq q-1$	$\mathcal{G}_{d+1}$	$q-1$
	$\widehat{W}_d = \langle \tau, \sigma^{\frac{1}{g-1}}\alpha_1\alpha_2, \epsilon^d\beta_1\rangle$	$1 \leq d \leq q-1$	$\mathcal{G}_{dk+1}$	$q-1$

Tabla 5.4: Representantes de subgrupos regulares del lema 5.1.10

Demostración. Todos los subgrupos G de la tabla son de la forma

$$G = \langle u, w\delta, \epsilon^c h\rangle, \tag{5.11}$$

donde $\langle u, w\rangle = \langle \sigma, \tau\rangle$, $\delta \in \langle \alpha_1, \alpha_2\rangle$, $c \neq 0$, $\delta(u) = u$, $\delta(w) = w$, $h(\epsilon) = \epsilon$. Por el lema 4.1.4(2), tenemos que $\langle \sigma, \tau\rangle \subseteq \pi_1(G)$. Dado que $\epsilon^c \in \pi_1(G)$, se tiene que $|\pi_1(G)| > p^2$ y en consecuencia $\pi_1(G) = \mathcal{G}_k$.

Un conjunto de representantes de las órbitas de los elementos de $\langle \sigma, \tau\rangle$ por la acción de $\operatorname{Aut}\mathcal{G}_k$ está dado por $\{\sigma, \tau, \sigma\tau\}$. Por lo tanto, los subgrupos con la misma imagen por π_2 y que pertenecen a distintas filas de la tabla no son conjugados entre sí puesto que sus núcleos con respecto a π_2 no lo son.

Supongamos que dos grupos de la misma fila son conjugados entre sí. Luego, sus proyecciones al cociente abeliano $\operatorname{Hol}(\mathcal{G}_k)/\mathfrak{H}_2$ coinciden. Por lo tanto, de acuerdo con (5.11), sus imágenes están generadas por $\epsilon^c h$ y $\epsilon^d h$ respectivamente y de esto se sigue que $c = d$.

Desarrollaremos el caso en el que la imagen por π_2 es $\mathcal{H}_{1,s}$. Para los demás casos se aplica la misma idea por lo que omitimos los cálculos.

Sea G un subgrupo regular de $\operatorname{Hol}(\mathcal{G}_k)$ con $\pi_2(G) = \mathcal{H}_{1,s}$. El núcleo de π_2 es un subgrupo de orden p de $\mathcal{G}_k$ y podemos fijarlo salvo por la acción del normalizador de $\mathcal{H}_{1,s}$ sobre los subgrupos de $\langle \sigma, \tau\rangle$.

Como $\{[(0,0),(a,b)] : 1 \leq a, b \leq p-1\} \leq N_{\operatorname{Aut}\mathcal{G}_k}(\mathcal{H}_{1,s})$, podemos suponer que el núcleo está generado por σ, por τ o por $\sigma\tau$. El grupo G tiene la forma

$$G = \langle u,\ v\epsilon^b\alpha_1,\ w\epsilon^d\beta_s\rangle$$

donde $u \in \{\sigma, \tau, \sigma\tau\}$ y $v, w \in \langle \sigma, \tau\rangle$. Por la condición (R): $(v\epsilon^b\alpha_1)^p \in \ker\pi_2 = \langle u\rangle$ tenemos que $(v\epsilon^b\alpha_1)^p\mathfrak{H}_2 = \epsilon^{bp}\mathfrak{H}_2 = \mathfrak{H}_2$ y entonces $b = 0$. Si $d = 0$ entonces de acuerdo con el lema 4.1.4(1), $\pi_1(G) \subseteq \langle \sigma, \tau\rangle$ y por lo tanto G no es regular. Luego, $d \neq 0$. Por la condición (R): $\beta_s\alpha_1\beta_s^{-1} = \alpha_1^g$ tenemos que

$$(w\epsilon^d\beta_s)v\alpha_1(w\epsilon^d\beta_s)^{-1} = (v\alpha_1)^g = v^g\alpha_1^g \pmod{\langle u\rangle}. \tag{5.12}$$

(i) Supongamos que $\ker\pi_2|_G = \langle \sigma\rangle$. Entonces G tiene la presentación estándar

$$G = \langle \sigma,\ \tau^a\alpha_1,\ \tau^c\epsilon^d\beta_s\rangle$$

para ciertos $a, d \neq 0$ y, salvo conjugación por $[(0,0),(1,a^{-1})]$, podemos asumir que $a = 1$. En consecuencia, G tiene la forma

$$G = \langle \sigma, \tau\alpha_1, \tau^c\epsilon^d\beta_s\rangle.$$

Por (5.12) tenemos

$$(\tau^c\epsilon^d\beta_s)\tau\alpha_1(\tau^c\epsilon^d\beta_s)^{-1} = \sigma^{g\frac{g^c-1}{g-1}}\tau^{g^{dk+s}}\alpha_1^g = \tau^g\alpha_1^g \pmod{\langle \sigma\rangle} \tag{5.13}$$

y se sigue que $d = \frac{1-s}{k}$ y por lo tanto $s \neq 1$. Si existe $h \in \operatorname{Aut}\mathcal{G}_k$ que normaliza a $\langle \sigma, \tau\alpha_1\rangle$ y tal que $h\tau^c\epsilon^{\frac{1-s}{k}}\beta_s h^{-1} \in \widehat{H}_{1,s}$, el grupo G es un conjugado de $\widehat{H}_{1,s}$. Luego, de acuerdo con (F_k) podemos elegir h como una potencia conveniente de α_1.

(ii) Supongamos ahora que $\ker \pi_2|_G = \langle \tau \rangle$. Entonces

$$G = \langle \tau, \sigma^a \alpha_1, \sigma^c \epsilon^d \beta_s \rangle$$

donde $a, d \neq 0$. En forma análoga al caso anterior, la ecuación (5.12) implica que $a = \frac{1}{g-1}$. Se cumple la relación $(\beta_s)^q = 1$ y entonces $(\sigma^c \epsilon^{-1} \beta_s)^q \in \langle \tau \rangle$. Por (P_k), si $d = -1$ entonces $(\sigma^c \epsilon^d \beta_s)^q = \sigma^{qc}$ y por lo tanto $c = 0$. En caso contrario, por (F_k), el grupo G es un conjugado de $\widetilde{H}_{1,s,d}$ mediante una potencia adecuada de α_1.

(iii) Supongamos, por último, que $\ker \pi_2|_G = \langle \sigma\tau \rangle$. Entonces

$$G = \langle \sigma\tau, \sigma^a \alpha_1, \sigma^c \epsilon^d \beta_s \rangle.$$

En forma análoga al caso (ii) tenemos que $a = \frac{1}{g-1}$, $d = \frac{s-1}{1-k} \neq 0$, $s \neq 1$ y si $d = -1$ entonces $c = 0$. Si $d \neq -1$, por (F_k) tenemos que G es un conjugado de $\overline{H}_{1,s}$ por una potencia adecuada de α_1. □

Lema 5.1.11. *Un conjunto de representantes de clases de equivalencia de subgrupos regulares G de $\mathrm{Hol}(\mathcal{G}_k)$ con $|\pi_2(G)| = p^2q$ está dado por la siguiente tabla:*

$\pi_2(G)$	*Subgrupos*	*Parámetros*	*Clase*	#
$\mathcal{T}_s$	$\widetilde{T}_{c,s} = \langle \sigma^{\frac{1}{g-1}} \alpha_1, \tau^{\frac{1}{g^k-1}} \alpha_2, \epsilon^c \beta_s \rangle$	$0 \leq s \leq q-1$ $1 \leq c \leq q-1$	$\mathcal{G}_s$	$q(q-1)$
	$\widehat{T}_s = \langle \sigma^{\frac{1}{g-1}} \alpha_1, \sigma\tau^{\frac{1}{g^k-1}} \alpha_2, \epsilon^{s-1} \beta_s \rangle$	$2 \leq s \leq q$	$\mathcal{G}_s$	$q-1$
	$\overline{T}_s = \langle \tau\sigma^{\frac{1}{g-1}} \alpha_1, \tau^{\frac{1}{g^k-1}} \alpha_2, \epsilon^{\frac{1-s}{k}} \beta_s \rangle$	$2 \leq s \leq q$	$\mathcal{G}_s$	$q-1$
$\mathcal{U}$	$\widetilde{U}_c = \langle \sigma^{\frac{1}{g-1}} \alpha_1, \tau^{\frac{1}{g^k-1}} \alpha_2, \epsilon^c \widetilde{\beta} \rangle$	$1 \leq c \leq q-1$	$\mathcal{G}_0$	$q-1$
	$\widehat{U} = \langle \tau\sigma^{\frac{1}{g-1}} \alpha_1, \tau^{\frac{1}{g^k-1}} \alpha_2, \epsilon^{-k^{-1}} \widetilde{\beta} \rangle$	-	$\mathcal{G}_0$	1
	$\overline{U} = \langle \sigma^{\frac{1}{g-1}} \alpha_1, \tau^{\frac{1}{g^k-1}} \sigma\alpha_2, \epsilon\widetilde{\beta} \rangle$	-	$\mathcal{G}_0$	1

Demostración. Los grupos que aparecen en diferentes filas de la tabla no son conjugados entre sí puesto que sus p-subgrupos de Sylow no lo son. Podemos aplicar el mismo argumento del lema 5.1.10 para mostrar que los grupos de la tabla son regulares y que los que pertenecen a una misma fila y comparten la misma imagen por π_2 no son conjugados entre sí (por ejemplo, si $\widetilde{T}_{c,s}$ y $\widetilde{T}_{d,s}$ son conjugados entonces $c = d$).

Sea G un subgrupo regular de $\mathrm{Hol}(\mathcal{G}_k)$ con $\pi_2(G) = \mathcal{T}_s$. Entonces

$$G = \langle u\epsilon^a \alpha_1, v\epsilon^b \alpha_2, w\epsilon^c \beta_s \rangle$$

para ciertos $u, v, w \in \langle \sigma, \tau \rangle$ y $0 \leq a, b, c \leq q-1$. Debemos verificar las condiciones (R) para los generadores de G. Como

$$(u\epsilon^a \alpha_1)^p = (v\epsilon^b \alpha_2)^p \overset{(R)}{=} 1,$$

entonces tenemos $(u\epsilon^a\alpha_1)^p\mathfrak{H}_2 = \epsilon^a\mathfrak{H}_2 = (v\epsilon^b\alpha_2)^p\mathfrak{H}_2 = \epsilon^b\mathfrak{H}_2$ y por lo tanto $a = b = 0$. Si $c = 0$, por el lema 4.1.4(1), $\pi_1(G) \subseteq \langle\sigma, \tau\rangle$ y entonces G no es regular. En consecuencia $c \neq 0$ y

$$(w\epsilon^c\beta_s)u\alpha_1(w\epsilon^c\beta_s)^{-1} \overset{(R)}{=} (u\alpha_1)^g = u^g\alpha_1^g, \tag{5.14}$$

$$(w\epsilon^c\beta_s)v\alpha_2(w\epsilon^c\beta_s)^{-1} \overset{(R)}{=} (v\alpha_2)^{g^s} = v^{g^s}\alpha_2^{g^s}. \tag{5.15}$$

La ecuación (5.14) implica que $u = \sigma^{\frac{1}{g-1}}\tau^n$ donde o bien $n = 0$ o bien $c = k^{-1}(1-s)$ y por la ecuación (5.15) tenemos que $v = \sigma^m\tau^{\frac{1}{g^k-1}}$ donde o bien $m = 0$ o bien $c = s - 1$. De la igualdad $c = k^{-1}(1-s) = s-1$ se deduce que $k = -1$ o $s = 1$. En ambos casos tenemos $c = 0$, una contradicción.

En consecuencia, debemos considerar los siguientes casos:

(i) $n = m = 0$.

(ii) $m = 0$, $c = k^{-1}(1-s)$, $n \neq 0$ y $s \neq 1$.

(iii) $n = 0$, $c = 1 - s$, $n \neq 0$ y $s \neq 1$.

Comencemos con (i):
Si $n = m = 0$ entonces

$$G = \langle\sigma^{\frac{1}{g-1}}\alpha_1, \tau^{\frac{1}{g^k-1}}\alpha_2, \sigma^a\tau^b\epsilon^c\beta_s\rangle$$

para ciertos a, b. Sea $h = \alpha_1^r\alpha_2^t$. Para conseguir $hGh^{-1} = \widetilde{T}_{c,s}$ para algún r, t, basta ver que $h\sigma^a\tau^b\epsilon^c\beta_s h^{-1} \in \widetilde{T}_{c,s}$. Por (F_k), esto es equivalente a que (r, t) sea una solución del sistema lineal:

$$\begin{cases} r(g^{c+1} - 1) = a(1-g) \\ t(1 - g^{ck+s}) = b(1-g^k). \end{cases}$$

Por (P_k) y la condición (R): $(\sigma^a\tau^b\epsilon^c\beta_s)^q = 1$, si $c + 1 = 0$ entonces $a = 0$ y si $ck + s = 0$ entonces $b = 0$. Por lo tanto, el sistema admite solución para todos a, b.

(ii) Sea $m = 0$ y $c = 1 - s$. Salvo conjugación por el automorfismo dado por $h = [(0,0), (n^{-1}, 1)]$ podemos suponer que $n = 1$. En consecuencia G tiene la forma

$$G = \langle\tau\sigma^{\frac{1}{g-1}}\alpha_1, \tau^{\frac{1}{g^k-1}}\alpha_2, \sigma^a\tau^b\epsilon^{\frac{1-s}{k}}\beta_s\rangle$$

para ciertos a, b. Sea (r, t) una solución del siguiente sistema lineal:

$$\begin{cases} r(g^{\frac{1-s+k}{k}} - 1) = a(1-g) \\ t(1-g) = b(1-g^k) + r(1-g^k)(1-g). \end{cases}$$

Tenemos $(\sigma^a\tau^b\epsilon^{\frac{1-s}{k}}\beta_s)^q = 1$. Gracias a (P_k), si $\frac{1-s}{k} + 1 = \frac{1-s+k}{k} = 0$ entonces $a = 0$. Luego, el sistema admite solución para todos a, b y entonces $\alpha_1^r\alpha_2^tG(\alpha_1^r\alpha_2^t)^{-1} = \widehat{T}_s$.

(iii) Sea $n = 0$ y $c = s - 1$. Salvo conjugación por $[(0,0),(1,m^{-1})]$ podemos asumir que $m = 1$, es decir

$$G = \langle \sigma^{\frac{1}{g-1}}\alpha_1, \sigma\tau^{\frac{1}{g^k-1}}\alpha_2, \sigma^a\tau^b\epsilon^{s-1}\beta_s \rangle$$

para ciertos a, b. Sea (r,t) una solución del siguiente sistema de ecuaciones:

$$\begin{cases} r(g^s-1) = (1-g^s)t + (1-g)a \\ t(g^{sk-k+s}-1) = (1-g^k)b. \end{cases}$$

Por la condición $(\sigma^a\tau^b\epsilon^{s-1}\beta_s)^q = 1$ y la ecuación (P_k) tenemos que si $sk-k+s = 0$ entonces $b = 0$ y si $s = 0$ entonces $a = 0$. En consecuencia, el sistema tiene solución y $\alpha_1^r\alpha_2^t G(\alpha_1^r\alpha_2^t)^{-1} = \overline{T}_s$.

En forma análoga, podemos tratar el caso $\pi_2(G) = \mathcal{U}$. En este caso, G es un conjugado de $\widetilde{U}_c$, $\widehat{U}$ o $\overline{U}$. □

Resumiendo el contenido de la subsección, tenemos la siguiente tabla:

$\lvert\ker\lambda\rvert$	$\mathbb{Z}_p^2 \times \mathbb{Z}_q$	$\mathcal{G}_k$	$\mathcal{G}_s,\ s \neq 0, \pm 1, k$	$\mathcal{G}_0$	$\mathcal{G}_{-1}$	$\mathcal{G}_1$
1	-	$2(q+1)$	$2(q+1)$	$2(q+1)$	$q+1$	$q-1$
p	2	$4(q+2)$	$4(q+2)$	$4(q+1)$	$2(q+2)$	$2(q-1)$
q	1	-	-	-	-	-
pq	-	-	-	4	-	-
p^2	1	$2q-3$	$2(q-1)$	$2(q-1)$	$q-1$	$q-1$
p^2q	-	1	-	-	-	-

Tabla 5.5: Enumeración de brazas torcidas de tipo $\mathcal{G}_k$ para $p = 1 \pmod q$.

5.1.3. Brazas torcidas de tipo $\mathcal{G}_0$

Consideremos el grupo $\mathcal{G}_0$ cuya presentación es

$$\mathcal{G}_0 = \langle \sigma, \tau, \epsilon \mid \sigma^p = \tau^p = \epsilon^q = [\sigma,\tau] = [\tau,\epsilon] = 1,\ \epsilon\sigma\epsilon^{-1} = \sigma^g \rangle.$$

De acuerdo con la descripción de los automorfismos de $\mathcal{G}_0$ dada en [17, Theorems 3.1, 3.4], la función

$$\phi : \mathbb{Z}_p \rtimes_\rho \left(\mathbb{Z}_p^\times \times \mathbb{Z}_p^\times\right) \longrightarrow \operatorname{Aut}\mathcal{G}_0, \quad [n,(a,b)] \mapsto h = \begin{cases} h|_{\langle\sigma,\tau\rangle} = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \\ \epsilon \mapsto \sigma^n\epsilon \end{cases}$$

donde $\rho(a,b)(n) = an$, es un isomorfismo de grupos.

En particular, $|\operatorname{Aut}\mathcal{G}_0| = p(p-1)^2$ y su p-subgrupo de Sylow está generado por $\alpha = [1,(1,1)]$.

Si G es un subgrupo regular de $\operatorname{Hol}(\mathcal{G}_0)$ entonces $|\pi_2(G)|$ divide a p^2q y a $|\operatorname{Aut}\mathcal{G}_0|$, luego divide a pq.

En esta sección utilizaremos los mismos cálculos de la subsección 5.1.2, teniendo en cuenta que en este caso el p-subgrupo de Sylow subgroup de $\operatorname{Aut}\mathcal{G}_0$ es cíclico y está generado por α.

Lema 5.1.12. *Un conjunto de representantes de clases de equivalencia de subgrupos regulares G de* $\operatorname{Hol}(\mathcal{G}_0)$ *con* $|\pi_2(G)| = p$ *es*

$$H = \langle \epsilon, \tau, \sigma^{\frac{1}{g-1}}\alpha \rangle \cong \mathbb{Z}_p^2 \times \mathbb{Z}_q, \quad K = \langle \epsilon, \sigma, \tau\alpha \rangle \cong \mathcal{G}_0.$$

Demostración. Podemos razonar de la misma forma que en el lema 5.1.6 teniendo en cuenta que los subgrupos de orden q de $\mathcal{G}_0$ están generados por elementos de la forma $\sigma^n\epsilon$. □

El subgrupo

$$\mathfrak{H}_3 = \langle \sigma, \tau, \alpha \rangle \tag{5.16}$$

es un subgrupo normal de $\mathrm{Hol}(\mathcal{G}_0)$ con $\mathrm{Hol}(\mathcal{G}_0)/\mathfrak{H}_3 \cong \mathbb{Z}_q \times \mathbb{Z}_p^\times \times \mathbb{Z}_p^\times$, se cumple la fórmula (P_k) en $\mathrm{Hol}(\mathcal{G}_0)$ tomando $k = 0$ y también la fórmula

$$\alpha^n u \epsilon^d \theta \alpha^{-n} = u \sigma^{xn\frac{g^d-1}{g-1}} \alpha^{(1-x)n} \epsilon^d \theta, \tag{F_0}$$

donde $u \in \langle \sigma, \tau \rangle$ y $\theta = [(0,0),(x,y)]$. Luego, por el mismo argumento de la proposición 5.1.8, tenemos la siguiente proposición.

Proposición 5.1.13. *Las brazas torcidas de tipo $\mathcal{G}_0$ con $|\ker \lambda| = p^2$ son $(B_{a,b}, +, \circ)$, donde $(B_{a,b}, +) = \mathbb{Z}_p^2 \rtimes_{\mathcal{D}_{1,0}} \mathbb{Z}_q$ y*

$$(B_{a,b}, \circ) = \mathbb{Z}_p^2 \rtimes_{\mathcal{D}_{a+1,b}} \mathbb{Z}_q \cong \begin{cases} \mathbb{Z}_p^2 \times \mathbb{Z}_q, & \text{si } a = q-1,\ b = 0, \\ \mathcal{G}_0, & \text{si } a = q-1,\ b \neq 0, \\ \mathcal{G}_{\frac{b}{a+1}}, & \text{en otro caso,} \end{cases}$$

para $0 \leq a, b \leq q-1$ y $(a,b) \neq (0,0)$. En particular, hay $q^2 - 1$ brazas torcidas bajo estas condiciones y todas ellas son bi-brazas.

En forma análoga al lema 5.1.9 obtenemos el siguiente conjunto de representantes de clases de conjugación de subgrupos de orden pq de $\mathrm{Aut}\,\mathcal{G}_0$:

$$\mathcal{H}_s = \langle \alpha, \beta_s \rangle, \quad \mathcal{K} = \langle \alpha, \widetilde{\beta} \rangle$$

donde $\beta_s = [0,(g,g^s)]$, $0 \leq s \leq q-1$ y $\widetilde{\beta} = [0,(1,g)]$.

Lema 5.1.14. *Un conjunto de representantes de subgrupos regulares G de $\mathrm{Hol}(\mathcal{G}_0)$ con $|\pi_2(G)| = pq$ está dado por la siguiente tabla:*

$\pi_2(G)$	*Subgrupos*	*Clase*	*Parámetros*	#
$\mathcal{H}_s$	$\widetilde{H}_{s,c} = \langle \tau, \sigma^{\frac{1}{g-1}}\alpha, \epsilon^c \beta_s \rangle$	$\mathcal{G}_s$	$0 \leq s \leq q-1$, $1 \leq c \leq q-1$	$q(q-1)$
	$\widehat{H}_s = \langle \sigma\tau, \sigma^{\frac{1}{g-1}}\alpha, \epsilon^{s-1}\beta_s \rangle$	$\mathcal{G}_s$	$2 \leq s \leq q$	$q-1$
$\mathcal{H}_1$	$\overline{H}_{1,c} = \langle \sigma, \tau\alpha, \epsilon^c \beta_1 \rangle$	$\mathcal{G}_{c+1}$	$1 \leq c \leq q-1$	$q-1$
$\mathcal{K}$	$\widetilde{K}_c = \langle \tau, \sigma^{\frac{1}{g-1}}\alpha, \epsilon^c \widetilde{\beta} \rangle$	$\mathcal{G}_0$	$1 \leq c \leq q-1$	$q-1$
	$\widehat{K} = \langle \sigma\tau, \sigma^{\frac{1}{g-1}}\alpha, \epsilon\widetilde{\beta} \rangle$	$\mathcal{G}_0$	-	1

Demostración. Por el mismo argumento del lema 5.1.10 podemos mostrar que los grupos de la tabla son regulares y que no son conjugados entre sí (en este caso, utilizaremos al grupo $\mathfrak{H}_3$ de (5.16)). Para ver que los grupos de la tabla forman un conjunto de representantes, podemos utilizar los mismos cálculos del lema 5.1.10 para los grupos cuya imagen por π_2 sea $\langle \alpha, \beta_s \rangle$ o $\langle \alpha, \widetilde{\beta} \rangle$.

Si suponemos que $\pi_2(G) = \mathcal{H}_s$ y $\ker \pi_2|_G = \langle \sigma \rangle$ la condición (R): (5.13) implica que $s = 1$. Para los demás casos podemos tomar $k = 0$ y utilizar los mismos cálculos.

Si suponemos que $\pi_2(G) = \mathcal{K}$ y $\ker \pi_2|_G = \langle \sigma \rangle$ entonces

$$G = \langle \sigma, \tau^a \alpha, \tau^b \epsilon^c \widetilde{\beta} \rangle$$

y por la misma condición tenemos que $a = 0$, es decir G no es regular. Los demás casos no sufren ninguna modificación.

Más aún, podemos usar (F_0) en lugar de (F_k) para mostrar que cualquier subgrupo regular G es un conjugado de alguno de la tabla utilizando una potencia adecuada de α. □

Observación 5.1.15. Una braza torcida B es un producto directo si y sólo si existen ideales I, J de B tales que $I + J = B$ y $I \cap J = 0$. El producto directo de una braza torcida de orden p^2 y de una de orden q es de tipo no abeliano. A continuación, mostramos las brazas torcidas de tipo $\mathcal{G}_0$ que son productos directos de la braza trivial de orden p y una braza torcida de orden pq. Como $\mathcal{G}_0$ es un producto directo de $\mathbb{Z}_p$ y $\mathbb{Z}_p \rtimes_g \mathbb{Z}_q$ sólo debemos considerar las brazas torcidas de orden pq con estructura aditiva no abeliana. Gracias a la clasificación del capítulo 3, hay $2q - 1$ brazas torcidas no triviales de las requeridas. Luego, debemos mostrar $2q - 1$ brazas torcidas que sean productos directos:

(i) Las brazas torcidas $B_{a,0}$ con $a \neq 0$ de la proposición 5.1.13 son productos directos de la braza trivial de orden p y de una braza torcida de orden pq con $|\ker \lambda| = p$.

(ii) La braza torcida asociada al grupo H del lema 5.1.12 es un producto directo de la braza trivial de orden p y de la única braza de orden pq con $|\ker \lambda| = q$.

(iii) Las brazas torcidas asociadas a $\widetilde{T}_{0,c}$ con $c \neq 0$ del lema 5.1.14 son productos directos de la braza trivial de orden p y de una braza torcida de orden pq con $|\ker \lambda| = 1$.

El contenido de esta subsección queda resumido en la siguiente tabla:

$\lvert\ker \lambda\rvert$	$\mathbb{Z}_p^2 \times \mathbb{Z}_q$	$\mathcal{G}_k, k \in \mathfrak{B} \setminus \{0, \pm 1\}$	$\mathcal{G}_0$	$\mathcal{G}_{-1}$	$\mathcal{G}_1$
p	-	$2(q+1)$	$2q+1$	$q+1$	$q-1$
pq	1	-	1	-	-
p^2	1	$2(q-1)$	$2q-3$	$q-1$	$q-1$
p^2q	-	-	1	-	-

Tabla 5.6: Enumeración de brazas torcidas de tipo $\mathcal{G}_0$ para $p = 1 \pmod q$.

5.1.4. Brazas torcidas de tipo $\mathcal{G}_{-1}$

Consideremos el grupo $\mathcal{G}_{-1}$ cuya presentación es

$$\mathcal{G}_{-1} = \langle \sigma, \tau, \epsilon \mid \sigma^p = \tau^p = \epsilon^q = [\sigma, \tau] = 1,\ \epsilon\sigma\epsilon^{-1} = \sigma^g,\ \epsilon\tau\epsilon^{-1} = \tau^{g^{-1}} \rangle.$$

Sea

$$\mathfrak{G} = \left(\mathbb{Z}_p^2 \rtimes_\rho (\mathbb{Z}_p^\times \times \mathbb{Z}_p^\times)\right) \rtimes_{\rho'} \mathbb{Z}_2$$

donde $\rho(a,b)(n,m) = (an, bm)$, $\rho'(1)[(n,m),(a,b)] = [(-gm, -g^{-1}n),(b,a)]$ para todos $0 \leq a, b, n, m \leq p-1$.

De acuerdo con [17, Subsections 4.1, 4.3], la función

$$\phi : \mathfrak{G} \longrightarrow \operatorname{Aut} \mathcal{G}_{-1}, \quad [(n,m),(a,b),i] \mapsto h = \begin{cases} h|_{\langle\sigma,\tau\rangle} = H_i(a,b), \\ \epsilon \mapsto \sigma^n \tau^m \epsilon^{(-1)^i}, \end{cases}$$

donde

$$H_0(a,b) = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}, \quad H_1(a,b) = \begin{bmatrix} 0 & a \\ b & 0 \end{bmatrix},$$

es un isomorfismo. La función

$$\nu : \operatorname{Aut} \mathcal{G}_{-1} \longrightarrow \mathbb{Z}_2, \quad [(n,m),(a,b),i] \mapsto i$$

es un morfismo de grupos y el grupo $\operatorname{Aut} \mathcal{G}_{-1}$ está generado por ${\operatorname{Aut} \mathcal{G}_{-1}}^+ = \ker \nu$ y por la involución $\psi = [(0,0),(1,1),1]$, definida por

$$\psi = \Big\{ \sigma \mapsto \tau, \quad \tau \mapsto \sigma, \quad \epsilon \mapsto \epsilon^{-1}. \tag{5.17}$$

Notemos que ${\operatorname{Aut} \mathcal{G}_{-1}}^+ \cong \operatorname{Aut} \mathcal{G}_k$ para $k \neq 0, \pm 1$ y contiene al p-subgrupo de Sylow de $\operatorname{Aut} \mathcal{G}_{-1}$, generado por $\alpha_1 = [(1,0),(1,1),0]$ y $\alpha_2 = [(0,1),(1,1),0]$, y los elementos de orden impar de $\operatorname{Aut} \mathcal{G}_{-1}$. Como $p > 2$, entonces $\pi_2(G) \leq {\operatorname{Aut} \mathcal{G}_{-1}}^+$ y $G \leq \mathcal{G}_{-1} \rtimes {\operatorname{Aut} \mathcal{G}_{-1}}^+ \leq \operatorname{Hol}(\mathcal{G}_{-1})$ para todo subgrupo regular $G \leq \operatorname{Hol}(\mathcal{G}_{-1})$. Sin embargo, las clases de conjugación de subgrupos regulares pueden ser diferentes, pues debemos tener en cuenta la conjugación por ψ.

En algunos casos, los cálculos para hallar las clases de conjugación se pueden copiar de la subsección 5.1.2 tomando $k = -1$, como en el siguiente caso que se sigue directamente del lema 5.1.7.

Lema 5.1.16. *La única braza torcida de tipo $\mathcal{G}_{-1}$ con $|\ker \lambda| = q$ es $(B, +, \circ)$ donde $(B,+) = \mathbb{Z}_p^2 \rtimes_{\mathcal{D}_{1,-1}} \mathbb{Z}_q$ y*

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \circ \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} x_1 g^{y_3} + y_1 g^{x_3} \\ x_2 g^{-y_3} + y_2 g^{-x_3} \\ x_3 + y_3 \end{pmatrix}$$

para todos $0 \leq x_1, x_2, y_1, y_2 \leq p-1$ y $0 \leq x_3, y_3 \leq q-1$.

En particular, $(B, \circ) \cong \mathbb{Z}_p^2 \times \mathbb{Z}_q$.

Las demostraciones del lema 5.1.6, la proposición 5.1.8, el lema 5.1.9 y el lema 5.1.10 sólo dependen de la condición $k \neq 0, 1$ por lo cual podemos utilizar estos resultados en las demostraciones siguientes. Notemos además que el subgrupo

$$\mathfrak{H}_4 = \langle \sigma, \tau, \alpha_1, \alpha_2 \rangle$$

es un subgrupo normal de $\mathrm{Hol}(\mathcal{G}_{-1})$ y tomando $k = -1$ en (F_k) obtenemos una fórmula válida en $\mathrm{Hol}(\mathcal{G}_{-1})$.

Lema 5.1.17. *Un conjunto de representantes de subgrupos regulares G de* $\mathrm{Hol}(\mathcal{G}_{-1})$ *con* $|\pi_2(G)| = p$ *es*

$$H_i = \langle \epsilon, \tau, \sigma^{\frac{1}{g-1}} \alpha_1 \alpha_2^i \rangle \cong \mathcal{G}_0$$

para $i = 0, 1$.

Demostración. Los grupos H_0 y H_1 no son conjugados entre sí pues sus imágenes por π_2 no lo son. Razonando como en el lema 5.1.6 podemos ver que todo subgrupo regular de $\mathrm{Hol}(\mathcal{G}_{-1})$ con $|\pi_2(G)| = p$ es un conjugado de los grupos H_i, K_i para $i = 0, 1$ que se definen tomando $k = -1$ en los grupos del lema 5.1.6. Es fácil ver que H_0 es un conjugado de K_0 por el automorfismo ψ y que H_1 es un conjugado de K_1 por el automorfismo $[(0,0),(g^2,1),0]$. □

Fijemos los automorfismos $\widetilde{\beta} = [(0,0),(1,g),0]$ y $\beta_s = [(0,0),(g,g^s),0]$ para $0 \leq s \leq q-1$.

Proposición 5.1.18. *Las brazas torcidas de tipo $\mathcal{G}_{-1}$ con $|\ker \lambda| = p^2$ están dadas por $(B_{a,b}, +, \circ)$ donde $(B_{a,b}, +) = \mathbb{Z}_p^2 \rtimes_{\mathcal{D}_{1,-1}} \mathbb{Z}_q$ y*

$$(B_{a,b}, \circ) = \mathbb{Z}_p^2 \rtimes_{\mathcal{D}_{a+1,b-1}} \mathbb{Z}_q \cong \begin{cases} \mathbb{Z}_p^2 \times \mathbb{Z}_q, & \text{si } a = q-1,\ b = 1, \\ \mathcal{G}_0, & \text{si } a = q-1,\ b \neq 1, \\ \mathcal{G}_{\frac{b-1}{a+1}}, & \text{en caso contrario,} \end{cases}$$

para $0 \leq a, b \leq q-1$ y $(a,b) \neq (0,0)$. En particular, son bi-brazas y $B_{a,b} \cong B_{c,d}$ si y sólo si $(c,d) = (-b,-a)$ y entonces tenemos $\frac{(q-1)(q+2)}{2}$ brazas torcidas con estas condiciones.

Demostración. Sea G un subgrupo regular de $\mathrm{Hol}(\mathcal{G}_{-1})$ tal que $|\pi_2(G)| = q$. Argumentando como en la proposición 5.1.8 podemos mostrar que todo grupo G es un conjugado de algún subgrupo

$$G_{a,b} = \langle \sigma, \tau, \epsilon \beta_0^a \widetilde{\beta}^b \rangle$$

por un elemento de $\mathrm{Aut}\,{\mathcal{G}_{-1}}^+$. Como $\psi G_{a,b} \psi = G_{-b,-a}$, los grupos de la forma $G_{a,-a}$ son normalizados por ψ y las demás órbitas son de tamaño 2. Por lo tanto, hay

$$q - 1 + \frac{q(q-1)}{2} = \frac{(q-1)(q+2)}{2}$$

órbitas bajo la acción de ψ. La afirmación acerca de la estructura de las brazas torcidas asociadas se sigue del mismo argumento que utilizamos en la proposición 5.1.8. □

Lema 5.1.19. *Un conjunto de representantes de clases de conjugación de subgrupos de* $\operatorname{Aut}\mathcal{G}_{-1}$ *de orden* pq *y* p^2q *está dado en la siguiente tabla:*

Orden	G	*Parámetros*	*Clase de isomorfismo*
pq	$\mathcal{H}_{1,s} = \langle \alpha_1, \beta_s \rangle$	$0 \leq s \leq q-1$	$\mathbb{Z}_p \rtimes_g \mathbb{Z}_q$
	$\mathcal{H}_{2,0} = \langle \alpha_2, \beta_0 \rangle$	-	$\mathbb{Z}_{pq}$
	$\mathcal{W} = \langle \alpha_1\alpha_2, \beta_1 \rangle$	-	$\mathbb{Z}_p \rtimes_g \mathbb{Z}_q$
p^2q	$\mathcal{T}_s = \langle \alpha_1, \alpha_2, \beta_s \rangle \cong \mathcal{G}_s$	$s \in \mathfrak{B}$	$\mathcal{G}_s$

donde $\mathfrak{B}$ *es el conjunto de la observación 4.2.5.*

Demostración. Los subgrupos de orden pq de $\operatorname{Aut}\mathcal{G}_{-1}{}^+$ salvo conjugación por elementos de $\operatorname{Aut}\mathcal{G}_{-1}{}^+$ son los del lema 5.1.9. Debemos calcular las órbitas de tales grupos bajo la acción de conjugación por ψ. Es fácil ver que

- $\psi\mathcal{H}_{1,s}\psi = \mathcal{H}_{2,s^{-1}}$ y $\psi\mathcal{T}_s\psi = \mathcal{T}_{s^{-1}}$ para $s \neq 0$;
- $\psi\mathcal{H}_{1,0}\psi = \mathcal{K}_2$, $\psi\mathcal{H}_{2,0}\psi = \mathcal{K}_1$ y $\psi\mathcal{U}\psi = \mathcal{T}_0$;
- $\psi\mathcal{W}\psi = \langle \alpha_1^{-g}\alpha_2^{-g^{-1}}, \beta_1 \rangle$ no es conjugado de ningún otro grupo de la tabla pues sus p-subgrupos de Sylow no son conjugados. □

Lema 5.1.20. *Un conjunto de representantes de clases de conjugación de subgrupos regulares* G *de* $\operatorname{Hol}(\mathcal{G}_{-1})$ *con* $|\pi_2(G)| = pq$ *está dado por la siguiente tabla:*

$\pi_2(G)$	*Subgrupos*	*Parámetros*	*Clase*	#
$\mathcal{H}_{1,s}$	$\widetilde{H}_{1,s,d} = \langle \tau, \sigma^{\frac{1}{g-1}}\alpha_1, \epsilon^d\beta_s \rangle$	$0 \leq s \leq q-1$, $1 \leq d \leq q-1$	$\mathcal{G}_{s-d}$	$q(q-1)$
	$\widehat{H}_s = \langle \sigma, \tau\alpha_1, \epsilon^{s-1}\beta_s \rangle$	$2 \leq s \leq q$	$\mathcal{G}_s$	$q-1$
	$\overline{H}_s = \langle \sigma\tau, \sigma^{\frac{1}{g-1}}\alpha_1, \epsilon^{\frac{s-1}{2}}\beta_s \rangle$	$2 \leq s \leq q$	$\mathcal{G}_{\frac{s+1}{2}}$	$q-1$
$\mathcal{H}_{2,0}$	$\widetilde{H}_{2,0,d} = \langle \sigma, \tau^{\frac{1}{g^{-1}-1}}\alpha_2, \epsilon^d\beta_0 \rangle$	$1 \leq d \leq q-1$	$\mathbb{Z}_p^2 \times \mathbb{Z}_q$, *si* $d = -1$ $\mathcal{G}_0$, *en otro caso*	$q-1$
	$\widehat{H}_{2,0} = \langle \tau, \sigma\alpha_2, \epsilon^{-1}\beta_0 \rangle$	-	$\mathcal{G}_0$	1
	$\overline{H}_{2,0} = \langle \sigma\tau, \tau^{\frac{1}{g^{-1}-1}}\alpha_2, \epsilon^{-\frac{1}{2}}\beta_0 \rangle$	-	$\mathcal{G}_0$	1
$\mathcal{W}$	$\widetilde{W}_d = \langle \sigma, \tau^{\frac{1}{g^{-1}-1}}\alpha_1\alpha_2, \epsilon^d\beta_1 \rangle$	$1 \leq d \leq q-1$	$\mathcal{G}_{d+1}$	$q-1$

Demostración. Sea G un subgrupo regular de $\operatorname{Hol}(\mathcal{G}_{-1})$ con $\pi_2(G) = \mathcal{H}_{i,s}$ con s, i como en el lema 5.1.19. Por los mismos cálculos del lema 5.1.10 podemos mostrar que G es un conjugado por algún elemento de $\operatorname{Aut}\mathcal{G}_{-1}{}^+$ de alguno de los grupos de la tabla con la misma imagen por π_2. Tales grupos no son conjugados. De hecho, si $\pi_2(G) \neq \mathcal{W}$, entonces su normalizador está contenido en $\operatorname{Aut}\mathcal{G}_{-1}{}^+ \cong \operatorname{Aut}\mathcal{G}_k$ para $k \neq 0, \pm 1$ y entonces podemos probar que los grupos correspondientes de la tabla no son conjugados como lo hicimos en el lema 5.1.10.

Si $\pi_2(G) = \mathcal{W}$, los grupos con $\pi_2(G) = \mathcal{W}$ son conjugados de $\widetilde{W}_d$ para algún $d \neq 0$ mediante algún elemento de $\operatorname{Aut}\mathcal{G}_{-1}{}^+$. Si $\widetilde{W}_c$ y $\widehat{W}_d$ son conjugados en $\operatorname{Aut}\mathcal{G}_{-1}$ por $h\psi$ para algún $h \in \operatorname{Aut}\mathcal{G}_{-1}{}^+$ entonces sus imágenes módulo el subgrupo $\mathfrak{H}_4$ también lo son. Por lo tanto, tenemos

$$h\psi\epsilon^c\beta_1\psi h^{-1}\mathfrak{H}_4 = \epsilon^{-c}\beta_1\mathfrak{H}_4 \in \langle\epsilon^d\beta_1\mathfrak{H}_4\rangle,$$

y entonces $c = -d$. Se puede ver que los grupos $\widetilde{W}_d$ y $\widehat{W}_{-d}$ son conjugados por $[(0,0),(1,g^2),0]$.

En consecuencia, la tabla presenta un conjunto de representantes de subgrupos regulares con las propiedades deseadas. □

Lema 5.1.21. *Un conjunto de representantes de clases de conjugación de subgrupos regulares G de* $\operatorname{Hol}(G_{-1})$ *con* $|\pi_2(G)| = p^2q$ *está dado por la siguiente tabla:*

$\pi_2(G)$	*Subgrupos*	*Clase*	*Parámetros*	$\#$
$\mathcal{T}_s$	$\widetilde{T}_{d,s} = \langle\sigma^{\frac{1}{g-1}}\alpha_1, \tau^{\frac{1}{g^{-1}-1}}\alpha_2, \epsilon^d\beta_s\rangle$	$\mathcal{G}_s$	$s \in \mathfrak{B}\setminus\{1\}$, $1 \leq d \leq q-1$	$\frac{q^2-1}{2}$
	$\widehat{T}_{m,s} = \langle\tau\sigma^{\frac{1}{g-1}}\alpha_1, \sigma^m\tau^{\frac{1}{g^{-1}-1}}\alpha_2, \epsilon^{s-1}\beta_s\rangle$	$\mathcal{G}_s$	$s \in \mathfrak{B}\setminus\{1,-1\}$, $0 \leq m \leq p-1$, $m \neq -\frac{g}{(g-1)^2} \pmod p$	$\frac{(p-1)(q-1)}{2}$
	$\overline{T}_s = \langle\sigma^{\frac{1}{g-1}}\alpha_1, \sigma\tau^{\frac{1}{g^{-1}-1}}\alpha_2, \epsilon^{s-1}\beta_s\rangle$	$\mathcal{G}_s$	$s \in \mathfrak{B}\setminus\{1,-1\}$	$\frac{q-1}{2}$
$\mathcal{T}_1$	$\widetilde{T}_{d,1} = \langle\sigma^{\frac{1}{g-1}}\alpha_1, \tau^{\frac{1}{g^{-1}-1}}\alpha_2, \epsilon^d\beta_1\rangle$	$\mathcal{G}_1$	$d \in \mathfrak{A}$	$\frac{q-1}{2}$
$\mathcal{T}_{-1}$	$\widehat{T}_{c,-1} = \langle\tau\sigma^{\frac{1}{g-1}}\alpha_1, \sigma^n\tau^{\frac{1}{g^{-1}-1}}\alpha_2, \epsilon^{-2}\beta_{-1}\rangle$	$\mathcal{G}_{-1}$	$0 \leq n \leq p-1$ $n \neq -\frac{g}{(g-1)^2} \pmod p$	$p-1$

donde $\mathfrak{A} \subseteq \mathbb{Z}_q^\times$ *contiene a un solo elemento de cada pareja* d *y* $-d$ *para todo* $d \in \mathbb{Z}_q^\times$.

Demostración. Usando el mismo argumento del lema 5.1.10 podemos mostrar que los grupos de la tabla son regulares. Veamos que los grupos con la misma imagen por π_2 en la tabla no son conjugados entre sí. Sea $\delta = h\psi$ para $h \in \operatorname{Aut}\mathcal{G}_{-1}{}^+$.

- Si $\pi_2(G) = \mathcal{T}_s$ y $s \neq \pm 1$ entonces $N_{\operatorname{Aut}\mathcal{G}_1}(\mathcal{T}_s) = \operatorname{Aut}\mathcal{G}_{-1}{}^+$. Luego, los grupos de diferentes filas y los de la familia $\widehat{T}_{m,s}$ no son conjugados entre sí pues sus p-subgrupos de Sylow no son conjugados por elementos de $\operatorname{Aut}\mathcal{G}_{-1}{}^+$.

- Si $s = 1$ entonces $\mathcal{T}_1$ es normal en $\operatorname{Aut}\mathcal{G}_{-1}$ y

  $$\delta\epsilon^c\beta_1\delta^{-1}\mathfrak{H}_4 = \psi\epsilon^c\beta_1\psi\mathfrak{H}_4 = \epsilon^{-c}\beta_1\mathfrak{H}_4.$$

  Luego, si $\widetilde{T}_{d,1}$ y $\widetilde{T}_{c,1}$ son conjugados por δ entonces necesariamente $c = -d$.

- Si $s = -1$ entonces $\mathcal{T}_{-1}$ es normal en $\operatorname{Aut}\mathcal{G}_{-1}$ y

  $$\delta\epsilon^c\beta_{-1}\delta^{-1}\mathfrak{H}_4 = \psi\epsilon^{-c}\beta_{-1}\psi\mathfrak{H}_4 = \epsilon^{-c}\beta_{-1}^{-1}\mathfrak{H}_4.$$

  Si $\widetilde{T}_{c,-1}$ y $\widetilde{T}_{d,-1}$ son conjugados por δ entonces $c = d$. Los grupos $\widetilde{T}_{c,-1}$ y $\widehat{T}_{n,-1}$ no son conjugados pues sus p-subgrupos de Sylow no lo son.

Sea G un subgrupo regular de $\mathrm{Hol}(\mathcal{G}_{-1})$. De acuerdo con el lema 5.1.19 podemos asumir que $\pi_2(G) = \mathcal{T}_s$ para $s \in \mathcal{B}$. Gracias a los mismos cálculos que hicimos al principio del lema 5.1.11, donde tomamos $k = -1$, tenemos que

$$G = \langle \sigma^{\frac{1}{g-1}}\tau^n\alpha_1,\ \sigma^m\tau^{\frac{1}{g^{-1}-1}}\alpha_2, w\epsilon^c\beta_s\rangle$$

para $c \neq 0$ y algún $w \in \langle\sigma, \tau\rangle$. Debemos discutir dos casos:

- $n = m = 0$;
- $(n, m) \neq (0, 0)$, $c = s - 1$ y entonces $s \neq 1$.

En el segundo caso, si $n = 0$ podemos fijar $m = 1$ utilizando la conjugación por $[(0, 0), (m^{-1}, m^{-1}), 0]$; en otro caso podemos fijar $n = 1$ utilizando la conjugación por $[(0, 0), (n^{-1}, n^{-1}), 0]$. Luego, redujimos los casos a $(n, m) = (0, 1)$ o $n = 1$ y $0 \leq m \leq p - 1$. Si $n = 1$ entonces los elementos $\tau\sigma^{\frac{1}{g-1}}$ y $\sigma^m\tau^{\frac{1}{g^{-1}-1}}$ deben ser linealmente independientes, es decir

$$det\begin{bmatrix} \frac{1}{g-1} & m \\ 1 & \frac{1}{g^{-1}-1}\end{bmatrix} = -\frac{g}{(g-1)^2} - m \neq 0 \pmod p.$$

En ambos casos, salvo conjugación por un elemento de $\langle\alpha_1, \alpha_2\rangle$ (utilizando (F_k) con $k = -1$) podemos suponer que $w = 1$ y entonces los subgrupos regulares se identifican con los parámetros (s, c, n, m).

Los grupos identificados con $(1, c, 0, 0)$ y $(1, -c, 0, 0)$ son conjugados por ψ. Los grupos identificados con $(-1, -2, 0, 1)$ y $(-1, -2, 1, 0)$ son conjugados entre sí por $[(0, 0), (1, -g), 0]\psi$. En consecuencia, G es un conjugado de alguno de los grupos de la tabla. □

Resumimos el contenido de esta subsección en la siguiente tabla:

$\lvert\ker\lambda\rvert$	$\mathbb{Z}_p^2 \times \mathbb{Z}_q$	$\mathcal{G}_k$	$\mathcal{G}_0$	$\mathcal{G}_{-1}$	$\mathcal{G}_1$
1	-	$p+q-1$	$p+q-1$	$p+q-2$	$\frac{q-1}{2}$
p	1	$2(q+2)$	$2(q+1)$	$q+2$	$q-1$
q	1	-	-	-	-
pq	-	-	2	-	-
p^2	1	$q-1$	$q-1$	$q-2$	$\frac{q-1}{2}$
p^2q	-	-	-	1	-

Tabla 5.7: Enumeración de las brazas torcidas de tipo $\mathcal{G}_{-1}$ para $p = 1 \pmod q$.

5.1.5. Brazas torcidas de tipo $\mathcal{G}_1$

Una presentación del grupo $\mathcal{G}_1$ es la siguiente

$$\mathcal{G}_1 = \langle\sigma, \tau, \epsilon \mid \sigma^p = \tau^p = \epsilon^q = [\sigma, \tau] = 1,\ \epsilon\sigma\epsilon^{-1} = \sigma^g,\ \epsilon\tau\epsilon^{-1} = \tau^g\rangle.$$

Por [17, Subsections 4.1, 4.2], la función

$$\phi : \mathbb{Z}_p^2 \rtimes GL_2(p) \longrightarrow \operatorname{Aut} \mathcal{G}_1, \quad [(n,m), H] \mapsto h = \begin{cases} h|_{\langle \sigma, \tau \rangle} = H, \\ \epsilon \mapsto \sigma^n \tau^m \epsilon \end{cases}$$

es un isomorfismo de grupos.

En particular, $|\operatorname{Aut} \mathcal{G}_1| = p^3(p-1)^2(p+1)$ y tenemos que un p-subgrupo de Sylow de $\operatorname{Aut} \mathcal{G}_1$ está generado por $\alpha_1 = [(1,0), Id]$, $\alpha_2 = [(0,1), Id]$, $\gamma = [(0,0), C]$, donde C es la matriz definida en la observación 4.2.5. Además, α_1 y α_2 generan un subgrupo normal en $\operatorname{Aut} \mathcal{G}_1$.

Notemos que para $k \neq 0, -1$ la función

$$\iota : \operatorname{Aut} \mathcal{G}_k \longrightarrow \operatorname{Aut} \mathcal{G}_1, \quad [(n,m),(a,b)] \mapsto \left[(n,m), \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}\right]$$

es un monomorfismo de grupos. Más aún, la fórmula (F_k) con $k = 1$ es válida en $\operatorname{Hol}(\mathcal{G}_1)$.

El procedimiento para verificar regularidad de un subgrupo es el mismo que utilizamos hasta ahora por lo cual comenzaremos a omitir la estrategia a partir de ahora salvo en los casos en que sea necesario.

Vamos a utilizar las fórmulas

$$\alpha_2 \gamma \alpha^{-1} \alpha_2^{-1} = \alpha_1^{-1} \gamma, \tag{5.18}$$

$$(\tau^a \alpha_2^b \gamma)^n = \sigma^{\frac{an(n-1)}{2}} \tau^{an} \alpha_1^{\frac{bn(n-1)}{2}} \alpha_2^{bn} \gamma^n \tag{5.19}$$

para $a, b, n \in \mathbb{Z}$.

Lema 5.1.22. *Un conjunto de representantes de clases de equivalencia de subgrupos regulares G de $\operatorname{Hol}(\mathcal{G}_1)$ con $|\pi_2(G)| = p$ es*

$$H = \langle \epsilon, \tau, \sigma^{\frac{1}{g-1}} \alpha_1 \rangle \cong \mathcal{G}_0, \quad W = \langle \epsilon, \sigma, \tau^{\frac{1}{g-1}} \alpha_2 \gamma \rangle \cong \mathcal{G}_0.$$

Demostración. Salvo conjugación, los subgrupos de orden p de $\operatorname{Aut} \mathcal{G}_1$ son $\langle \alpha_1 \rangle$, $\langle \alpha_2^i \gamma \rangle$ para $i = 1, 2$. Por lo tanto, H y W no son conjugados.

Si $\pi_2(G) = \langle \alpha_1 \rangle$, por el mismo argumento del lema 5.1.6 podemos mostrar que G es un conjugado de H.

Sea G un subgrupo regular de $\operatorname{Hol}(\mathcal{G}_1)$ con $\pi_2(G) = \langle \alpha_2^i \gamma \rangle$ para $i = 0, 1$. Entonces $K = \ker \pi_2|_G$ contiene un elemento de orden q y entonces, salvo conjugación por una potencia de α_1, podemos asumir que K está generado por un elemento de la forma $\tau^n \epsilon$ y por algún $v \in \langle \sigma, \tau \rangle$. Luego, G tiene la siguiente presentación estándar:

$$G = \langle \tau^n \epsilon, v, u \alpha_2^i \gamma \rangle$$

donde $u, v \in \langle \sigma, \tau \rangle$. Como el p-subgrupo de Sylow de K es característico en K y K es normal en G entonces $\langle v \rangle$ es normal en G. Luego

$$w \alpha_2^i \gamma(u) w^{-1} = \gamma(u) \in \langle u \rangle.$$

En consecuencia, podemos asumir que $u = \sigma$ y entonces $u = \tau^c$ para $c \neq 0$. Por la condición (K), tenemos

$$\tau^c \alpha_2^i \gamma \tau^n \epsilon \gamma^{-1} \alpha_2^{-i} \tau^{-c} = \sigma^n \tau^{(1-g)c+i+n} \epsilon \in K.$$

Luego, $(1-g)c+i = 0$. Si $i = 0$ entonces $c = 0$ y en consecuencia G no es regular. Por lo tanto, $i = 1$ y $c = \frac{1}{g-1}$. Por último, usando (5.18), tenemos que G es conjugado de W por $\alpha_2^{-n}\gamma^{-n}$. □

Lema 5.1.23. *Un conjunto de representantes de clases de equivalencia de subgrupos regulares G de* $\mathrm{Hol}(\mathcal{G}_1)$ *con* $|\pi_2(G)| = p^2$ *es*

$$H_i = \langle \epsilon,\, \sigma^{\frac{1}{g-1}} \alpha_1,\, \tau^{\frac{1}{g-1}} \alpha_2 \gamma^i \rangle \cong \mathbb{Z}_p^2 \times \mathbb{Z}_q$$

para $i = 0, 1$.

Demostración. Los subgrupos de $\operatorname{Aut} \mathcal{G}_1$ de orden p^2 son $\langle \alpha_1, \alpha_2 \rangle$, $\langle \alpha_1, \gamma \rangle$ y $\langle \alpha_1, \alpha_2 \gamma \rangle$, salvo conjugación. Entonces, los grupos del enunciado no son conjugados entre sí pues sus imágenes por π_2 no lo son.

Sea G un subgrupo regular de $\mathrm{Hol}(\mathcal{G}_1)$ tal que $|\pi_2(G)| = p^2$. El núcleo de π_2 es el único q-subgrupo de Sylow de G por lo cual G es abeliano. Más aún, salvo conjugación por el normalizador de $\pi_2(G)$ podemos suponer que está generado por ϵ.

Si $\pi_2(G) = \langle \alpha_1, \alpha_2 \rangle$ entonces G es un conjugado de H_0 por un elemento de $\iota(\operatorname{Aut} \mathcal{G}_k) \leq \operatorname{Aut} \mathcal{G}_1$ (véase el lema 5.1.7). En caso contrario, tenemos que

$$G = \langle \epsilon, u\alpha_1, v\alpha_2^i \gamma \rangle$$

para ciertos $u, v \in \langle \sigma, \tau \rangle$. Dado que G es abeliano se sigue que $u = \sigma^{\frac{1}{g-1}}$ y $v = \tau^{\frac{i}{g-1}}$ por (5.18). Como $v \neq 1$ entonces $i = 1$ y por lo tanto $G = H_1$. □

Utilizando la misma notación de la observación 4.2.5 definimos $\widetilde{\beta} = [(0,0), \mathcal{D}_{0,1}]$ y $\beta_s = [(0,0), \mathcal{D}_{1,s}]$ para $1 \leq s \leq q-1$.

Proposición 5.1.24. *Las brazas torcidas de tipo $\mathcal{G}_1$ con $|\ker \lambda| = p^2$ son $(B_{a,b}, +, \circ)$ donde $(B_{a,b}, +) = \mathbb{Z}_p^2 \rtimes_{\mathcal{D}_{1,1}} \mathbb{Z}_q$ y*

$$(B_{a,b}, \circ) = \mathbb{Z}_p^2 \rtimes_{\mathcal{D}_{a+1,b+1}} \mathbb{Z}_q \cong \begin{cases} \mathbb{Z}_p^2 \times \mathbb{Z}_q, & \text{si } a = b = q-1, \\ \mathcal{G}_0, & \text{si } a = q-1,\ b \neq q-1, \\ \mathcal{G}_{\frac{b+1}{a+1}}, & \text{caso contrario,} \end{cases}$$

para $0 \leq a, b \leq q-1$ y $(a,b) \neq (0,0)$. Más aún, son bi-brazas y $B_{a,b} \cong B_{c,d}$ si y sólo si $(c,d) = (b,a)$ y entonces hay $\frac{(q-1)(q+2)}{2}$ de tales brazas torcidas.

Demostración. Sea G un subgrupo regular de $\mathrm{Hol}(\mathcal{G}_1)$ tal que $|\pi_2(G)| = q$. Por la observación 4.2.5 tenemos que, salvo conjugación, un elemento de orden q de $GL_2(p)$ es una matriz diagonal cuyas entradas son potencias de g. Argumentando como en

la proposición 5.1.8, también en este caso podemos mostrar que G es un conjugado de algún subgrupo de la forma

$$G_{a,b} = \langle \sigma, \tau, \epsilon\beta_0^a\widetilde{\beta}^b\rangle.$$

Luego $G_{a,b}$ y $G_{c,d}$ son conjugados por $h \in \operatorname{Aut}\mathcal{G}_1$ si y sólo si

$$h(\epsilon)h\beta_0^a\widetilde{\beta}^b h^{-1} = \epsilon h\beta_0^a\widetilde{\beta}^b h^{-1} = \epsilon\beta_0^c\widetilde{\beta}^d \pmod{\langle\sigma,\tau\rangle},$$

es decir, $\beta_0^a\widetilde{\beta}^b|_{\langle\sigma,\tau\rangle} = \mathcal{D}_{a,b}$ y $\beta_0^c\widetilde{\beta}^d|_{\langle\sigma,\tau\rangle} = \mathcal{D}_{c,d}$ son conjugados.

Además, o bien $(a,b) = (c,d)$ o bien $(a,b) = (d,c)$. En particular hay $\frac{(q-1)(q+2)}{2}$ de tales clases. El resto se sigue al igual que en la proposición 5.1.8. □

El siguiente lema resume las clases de conjugación de los subgrupos de orden pq y p^2q de $\operatorname{Aut}\mathcal{G}_1$.

Lema 5.1.25. *Un conjunto de representantes de clases de equivalencia de subgrupos de orden pq y p^2q de $\operatorname{Aut}\mathcal{G}_1$ es*

Orden	G	*Parámetros*	*Clase*
pq	$\mathcal{H}_s = \langle\alpha_1, \beta_s\rangle$	$0 \le s \le q-1$	$\mathbb{Z}_p \rtimes_g \mathbb{Z}_q$
	$\mathcal{U} = \langle\alpha_2, \beta_0\rangle$	-	$\mathbb{Z}_{pq}$
	$\mathcal{K}_s = \langle\gamma, \beta_s\rangle$	$0 \le s \le q-1$	$\mathbb{Z}_{pq}$, *si* $s = 1$, $\mathbb{Z}_p \rtimes_g \mathbb{Z}_q$, *en otro caso*
	$\mathcal{M} = \langle\alpha_1\alpha_2^2\gamma, \beta_{2^{-1}}\rangle$	-	$\mathbb{Z}_p \rtimes_g \mathbb{Z}_q$
	$\mathcal{V} = \langle\gamma, \widetilde{\beta}\rangle$	-	$\mathbb{Z}_p \rtimes_g \mathbb{Z}_q$
p^2q	$\mathcal{T}_s = \langle\alpha_1, \alpha_2, \beta_s\rangle$	$s \in \mathfrak{B}$	$\mathcal{G}_s$
	$\mathcal{R}_s = \langle\alpha_1, \gamma, \beta_s\rangle$	$0 \le s \le q-1$	$\mathcal{G}_{1-s}$
	$\mathcal{N} = \langle\alpha_1, \gamma, \widetilde{\beta}\rangle$	-	$\mathcal{G}_0$
	$\mathcal{L} = \langle\alpha_1, \alpha_2\gamma, \beta_{2^{-1}}\rangle$	-	$\mathcal{G}_2$

donde $\mathfrak{B}$ es como en la sección 4.2.

Demostración. Los grupos de la tabla no son conjugados entre sí. En efecto, si $h = [(n,m), M]$ conjuga a un par de grupos de la tabla entonces sus p-subgrupos de Sylow son conjugados por h y sus restricciones a $\langle\sigma,\tau\rangle$ son conjugados por M. Un análisis caso por caso muestra que estas dos condiciones no pueden cumplirse para ningún par de grupos de la tabla.

Sea H un subgrupo de orden pq o p^2q de $\operatorname{Aut}\mathcal{G}_1$ y sea $H|_{\langle\sigma,\tau\rangle}$ la restricción de la acción de H a $\langle\sigma,\tau\rangle$. Si $H|_{\langle\sigma,\tau\rangle}$ tiene orden q entonces, por la observación 4.2.5 tenemos que $H|_{\langle\sigma,\tau\rangle}$ está generado por $\mathcal{D}_{1,s}$ para $s \in \mathcal{B}$. Luego, salvo conjugación, $H \le \iota(\operatorname{Aut}\mathcal{G}_k)$. Utilizando la misma notación del lema 5.1.9, tenemos que H es un conjugado de alguno de los grupos $\{\mathcal{H}_{1,s}, \mathcal{H}_{2,s}, \mathcal{W}, \mathcal{T}_s : s \in \mathcal{B}\}$ por un elemento de $\iota(\operatorname{Aut}\mathcal{G}_k)$. Más aún:

- Si $s \neq 0, \pm 1$, $\psi \mathcal{H}_{1,s} \psi = \mathcal{H}_{2,s^{-1}}$, donde ψ es el automorfismo que intercambia σ con τ.
- el grupo $\mathcal{W}$ es conjugado de $\mathcal{H}_{1,1}$ por un automorfismo de la forma $[(0,0), M]$, pues $\mathcal{D}_{1,1}$ es central en $GL_2(p)$.

Por lo tanto H es un conjugado de alguno de los grupos $\{\mathcal{H}_s, \mathcal{U} : 0 \leq s \leq q-1\}$ si $|H| = pq$ o de alguno de los grupos $\{\mathcal{T}_s : 0 \leq s \leq q-1\}$ si $|H| = p^2q$ como afirmamos en el enunciado.

Si $H|_{\langle \sigma, \tau \rangle}$ tiene orden pq entonces, por la observación 4.2.5, salvo conjugación tenemos que $H|_{\langle \sigma, \tau \rangle} = \langle C, \mathcal{D}_{1,s} \rangle$ o $H|_{\langle \sigma, \tau \rangle} = \langle C, \mathcal{D}_{0,1} \rangle$ para $0 \leq s \leq q-1$. Por lo tanto

$$H = \langle \alpha_1^n \alpha_2^m \gamma,\ \alpha_1^r \alpha_2^t \theta \rangle$$

para $\theta \in \{\beta_s, \widetilde{\beta} : 0 \leq s \leq q-1\}$. Si $\theta = \beta_0$ entonces $t = 0$ y si $\theta = \widetilde{\beta}$ entonces $r = 0$. Usando (F_k) para $k = 1$, salvo conjugación podemos asumir que $r = t = 0$. El p-subgrupo de Sylow de H debe ser normal, es decir si $\theta = [(0,0), \mathcal{D}_{t,s}]$, usando (5.19) tenemos que

$$\theta \alpha_1^n \alpha_2^m \gamma \theta^{-1} = \alpha_1^{ng^t} \alpha_2^{mg^s} \gamma^{g^{t-s}} = (\alpha_1^n \alpha_2^m \gamma)^r = \alpha_1^{nr + mr\frac{r-1}{2}} \alpha_2^{mr} \gamma^r$$

para cierto $r \in \mathbb{Z}$. Luego, $r = g^{s-t}$ y n, m satisfacen las ecuaciones del siguiente sistema lineal:

$$\begin{cases} 2(g^{t-s} - g^t)n + g^{t-s}(g^{t-s} - 1)m = 0 \\ (g^{t-s} - g^s)m = 0. \end{cases}$$

En consecuencia:

- si $\theta = \beta_s, \widetilde{\beta}$ con $s \neq 0, 2^{-1}$ entonces $n = m = 0$, es decir $H = \mathcal{K}_s$ o $H = \mathcal{V}$;
- si $\theta = \beta_{2^{-1}}$ entonces $m = 2n$ y por lo tanto, o bien $n = m = 0$ o bien, salvo conjugación por $[(0,0), n^{-1}Id]$, $n = 1, m = 2$, es decir $H = \mathcal{K}_{2^{-1}}$ o H es un conjugado de $\mathcal{M}$;
- si $\theta = \beta_0$ entonces o bien $n = m = 0$ o bien, salvo conjugación por el automorfismo $[(0,0), n^{-1}Id]$, $m = 0$ y $n = 1$. Puesto que $\alpha_2 \langle \alpha_1 \gamma, \beta_0 \rangle \alpha_2^{-1} = \mathcal{K}_0$ entonces H es un conjugado de $\mathcal{K}_0$.

Sea H un subgrupo de $\operatorname{Aut} \mathcal{G}_1$ de orden p^2q y sea $H|_{\langle \sigma, \tau \rangle}$ de orden pq. Entonces, salvo conjugación,

$$H = \langle \alpha_1^n \alpha_2^m,\ \alpha_1^r \alpha_2^t \gamma,\ \theta \rangle$$

donde θ es o bien β_s o bien $\widetilde{\beta}$. Usando (5.18) para verificar abelianidad del p-subgrupo de Sylow de H se sigue que $m = 0$ y entonces podemos suponer que $n = 1$ y $r = 0$. Dado que el p-subgrupo de Sylow es abeliano, se sigue que:

- si $\theta = \beta_s$ para $s \neq 2^{-1}$ entonces $t(g^s - g^{1-s}) = 0$ y luego $t = 0$, es decir $H = \mathcal{R}_s$;
- si $\theta = \widetilde{\beta}$ entonces $(1-g)t = 0$ y luego $t = 0$, es decir $H = \mathcal{N}$;

- si $\theta = \beta_{2^{-1}}$ entonces salvo conjugación por un elemento de la forma $[(0,0), xId]$ tenemos $t \in \{0,1\}$, es decir H es un conjugado o bien de $\mathcal{R}_{2^{-1}}$ o bien de $\mathcal{L}$.

□

El grupo

$$\mathfrak{H}_5 = \langle \sigma, \tau, \alpha_1, \alpha_2 \rangle \tag{5.20}$$

es un subgrupo normal de $\mathrm{Hol}(\mathcal{G}_1)$ y $\mathrm{Hol}(\mathcal{G}_1)/\mathfrak{H}_5 \cong \mathbb{Z}_q \times GL_2(p)$.

Lema 5.1.26. *Un conjunto de representantes de clases de conjugación de subgrupos regulares G de* $\mathrm{Hol}(\mathcal{G}_1)$ *con* $|\pi_2(G)| = pq$ *es*

$\pi_2(G)$	*Subgrupos*	*Parámetros*	*Clase*	#
$\mathcal{H}_s$	$\widetilde{H}_{s,c} = \langle \tau, \sigma^{\frac{1}{g-1}}\alpha_1, \epsilon^c\beta_s \rangle$	$0 \le s \le q-1$, $1 \le c \le q-1$	$\mathcal{G}_{c+s}$	$q(q-1)$
	$\widehat{H}_s = \langle \sigma, \tau\alpha_1, \epsilon^{1-s}\beta_s \rangle$	$2 \le s \le q$	$\mathcal{G}_{2-s}$	$q-1$
$\mathcal{K}_s$	$\widetilde{K}_s = \langle \sigma, \tau\gamma, \epsilon^{1-2s}\beta_s \rangle$	$0 \le s \le q-1$, $s \neq 2^{-1}$	$\mathbb{Z}_p^2 \times \mathbb{Z}_q$, *si* $s = 1$, $\mathcal{G}_2$, *en caso contrario.*	$q-1$
$\mathcal{U}$	$\widetilde{U}_c = \langle \sigma, \tau^{\frac{1}{g-1}}\alpha_2, \epsilon^c\beta_0 \rangle$	$1 \le c \le q-1$	$\mathbb{Z}_p^2 \times \mathbb{Z}_q$, *si* $c = -1$, $\mathcal{G}_0$, *en caso contrario.*	$q-1$
	$\widetilde{U} = \langle \tau, \sigma\alpha_2, \epsilon^{-1}\beta_0 \rangle$	-	$\mathcal{G}_0$	1
$\mathcal{M}$	$\widetilde{M}_c = \langle \sigma, \tau^{\frac{2}{g-1}}\alpha_1\alpha_2^2\gamma, \epsilon^c\beta_{2^{-1}} \rangle$	$1 \le c \le q-1$	$\mathcal{G}_{2(c+1)}$	$q-1$
$\mathcal{V}$	$\widetilde{V} = \langle \sigma, \tau\gamma, \epsilon^{-2}\widetilde{\beta} \rangle$	-	$\mathcal{G}_2$	1

Demostración. Los grupos con la misma imagen por π_2 pero de diferentes filas de la tabla no son conjugados entre sí puesto que sus p-subgrupos de Sylow no son conjugados por el normalizador de su imagen por π_2. El mismo argumento del lema 5.1.10 nos dice que los grupos de la misma fila no son conjugados entre sí (utilizando al grupo $\mathfrak{H}_5$).

Sea G un subgrupo regular de $\mathrm{Hol}(\mathcal{G}_1)$ con $\pi_2(G) \in \{\mathcal{H}_s, \mathcal{U} : 0 \le s \le q-1\}$, es decir con $\pi_2(G) \le \iota(\mathrm{Aut}\,\mathcal{G}_k)$. Entonces $G \le \mathcal{G}_1 \rtimes \iota(\mathrm{Aut}\,\mathcal{G}_k)$ y podemos suponer que

$$G = \langle u, v\alpha_i, w\epsilon^c\beta_s \rangle$$

para ciertos $c \neq 0$ y $u, v, w \in \langle \sigma, \tau \rangle$. Salvo conjugación por un elemento del normalizador de $\pi_2(G)$ podemos suponer que $u \in \{\sigma, \tau, \sigma\tau\}$.

Si $\ker \pi_2 = \langle \sigma\tau \rangle$, la condición (K) implica que $s = 1$ y $i = 1$. En tal caso, salvo conjugación por $h \in N_{\mathrm{Aut}\,\mathcal{G}_1}(\mathcal{H}_1)$, podemos suponer que el núcleo está generado por σ.

En consecuencia, reemplazando $k = 1$ en la demostración del lema 5.1.10, se sigue que G es un conjugado de alguno de los grupos de la tabla con la misma imagen por π_2 salvo conjugación por un elemento de $\iota(\mathrm{Aut}\,\mathcal{G}_k)$ (estamos usando que (F_k) y (P_k) son válidas para $k = 1$).

En los demás casos podemos suponer que G tiene la forma

$$G = \langle u, v\alpha_1^n\alpha_2^m\gamma, w\epsilon^c\theta\rangle$$

para ciertos $c \neq 0$ y $u, v, w \in \langle\sigma, \tau\rangle$. Por la condición (K) tenemos que $\ker \pi_2|_G = \langle\sigma\rangle$ y luego $v, w \in \langle\tau\rangle$.

Sea $\pi_2(G) = \mathcal{K}_s$. Entonces

$$G = \langle\sigma,\ \tau^a\gamma,\ \tau^b\epsilon^c\beta_s\rangle$$

para $a \neq 0$ y entonces, salvo conjugación por $h = [(0,0), a^{-1}Id]$ podemos asumir que $a = 1$. En $\mathcal{K}_s$ se satisface la relación $\beta_s\gamma\beta_s^{-1} = \gamma^{g^{1-s}}$. Entonces la condición (R) y la fórmula (5.19) implican que

$$(\tau^b\epsilon^c\beta_s)\tau\gamma(\tau^b\epsilon^c\beta_s)^{-1} = \tau^{g^{s+c}}\gamma^{g^{1-s}} \overset{(R)}{=} (\tau\gamma)^{g^{1-s}} = \tau^{g^{1-s}}\gamma^{g^{1-s}} \quad (\text{mód } \langle\sigma\rangle)$$

y luego $c = 1 - 2s$; en consecuencia, $s \neq 2^{-1}$. Como $(\tau^b\epsilon^{1-2s}\beta_s)^q \in \ker\pi_2$, si $s = 1$ entonces $b = 0$ (ver (P_k)). En otro caso, G es un conjugado de $\widetilde{K}_s$ por γ^n donde $n = \frac{b}{1-g^{1-s}}$.

Los otros casos son análogos por lo cual omitimos los cálculos. □

Lema 5.1.27. *Un conjunto de representantes de clases de conjugación de subgrupos regulares G de* $\mathrm{Hol}(\mathcal{G}_1)$ *con* $|\pi_2(G)| = p^2q$ *es*

$\pi_2(G)$	*Subgrupos*	*Parámetros*	*Clase*	$\#$
$\mathcal{T}_s$	$\widetilde{T}_{s,d} = \langle\sigma^{\frac{1}{g-1}}\alpha_1, \tau^{\frac{1}{g-1}}\alpha_2, \epsilon^d\beta_s\rangle$	$s \in \mathfrak{B} \setminus \{-1\}$, $1 \leq d \leq q-1$	$\mathcal{G}_s$	$\frac{(q-1)(q+1)}{2}$
	$\widetilde{T}_{-1,d} = \langle\sigma^{\frac{1}{g-1}}\alpha_1, \tau^{\frac{1}{g-1}}\alpha_2, \epsilon^d\beta_{-1}\rangle$	$d \in \mathfrak{A}$	$\mathcal{G}_{-1}$	$\frac{q-1}{2}$
	$\widehat{T}_s = \langle\sigma^{\frac{1}{g-1}}\alpha_1, \sigma\tau^{\frac{1}{g-1}}\alpha_2, \epsilon^{s-1}\beta_s\rangle$	$s \in \mathfrak{B} \setminus \{1\}$	$\mathcal{G}_s$	$\frac{q+1}{2}$
	$\overline{T}_s = \langle\tau\sigma^{\frac{1}{g-1}}\alpha_1, \tau^{\frac{1}{g-1}}\alpha_2, \epsilon^{1-s}\beta_s\rangle$	$s \in \mathfrak{B} \setminus \{1, -1\}$	$\mathcal{G}_s$	$\frac{q-1}{2}$
$\mathcal{R}_s$	$\widetilde{R}_s = \langle\sigma^{\frac{1}{g-1}}\alpha_1, \tau\gamma, \tau^{\frac{1-g^{1-s}}{2}}\epsilon^{1-2s}\beta_s\rangle$	$0 \leq s \leq q-1,\ s \neq 2^{-1}$	$\mathcal{G}_{1-s}$	$q-1$
$\mathcal{N}$	$\widetilde{N} = \langle\sigma^{\frac{1}{g-1}}\alpha_1, \tau\gamma, \tau^{\frac{1-g^{-1}}{2}}\epsilon^{-2}\widetilde{\beta}\rangle$	-	$\mathcal{G}_0$	1
$\mathcal{L}$	$\widetilde{L}_d = \langle\sigma^{\frac{1}{g-1}}\alpha_1, \tau^{\frac{1}{g-1}}\alpha_2\gamma, \epsilon^d\beta_{2^{-1}}\rangle$	$1 \leq d \leq q-1$	$\mathcal{G}_2$	$q-1$

donde $\mathfrak{A}$ es el conjunto del lema 5.1.21.

Demostración. Veamos primero que los grupos de la tabla no son conjugados entre sí:

- con $s \neq -1$, si $\widehat{T}_{s,d}$ (resp. $\widetilde{L}_d$) y $\widehat{T}_{s,c}$ (resp. $\widetilde{L}_c$) son conjugados por algún elemento del normalizador de sus imágenes por π_2 entonces, comparando las imágenes en el cociente $\mathrm{Hol}(\mathcal{G}_1)/\mathfrak{H}_5$ se sigue que $c = d$ (el mismo argumento muestra que los grupos $\widehat{T}_s$ y $\overline{T}_s$ para $s \neq -1$ y los grupos $\widetilde{L}_d$ no son conjugados entre sí). Si $s = -1$ el mismo argumento muestra que $c = -d$.

- si $\pi_2(G) = \mathcal{T}_s$ para $s \neq \pm 1$ entonces la acción de $h \in N_{\operatorname{Aut}\mathcal{G}_1}(\pi_2(G))$ restringida a $\langle \sigma, \tau \rangle$ es una matriz diagonal. Por lo tanto, los grupos $\widetilde{T}_{s,d}$, $\widehat{T}_s$ y $\overline{T}_s$ no son conjugados puesto que sus p-subgrupos de Sylow no lo son.

- si $s \neq -1$ y $\widetilde{T}_{s,d}$ y $\widetilde{T}_{s,c}$ son conjugados entonces, comparando sus imágenes en el cociente $\operatorname{Hol}(\mathcal{G}_1)/\mathfrak{H}_5$ se sigue que $c = d$ (el mismo argumento muestra que los grupos $\widehat{T}_s$ y $\overline{T}_s$ para $s \neq -1$ y los grupos $\widetilde{L}_d$ no son conjugados entre sí).

- si $\pi_2(G) = \mathcal{T}_{-1}$ entonces la acción de $h \in N_{\operatorname{Aut}\mathcal{G}_1}(\pi_2(G))$ restringida a $\langle \sigma, \tau \rangle$ es un matriz diagonal o bien tiene la forma

$$h|_{\langle \sigma,\tau \rangle} = \begin{bmatrix} 0 & b \\ a & 0 \end{bmatrix}.$$

  Los grupos $\widehat{T}_{-1}$ y $\overline{T}_{-1}$ y los grupos $\widetilde{T}_{-1,c}$ y $\widetilde{T}_{-1,-c}$ son conjugados por el automorfismo ψ que intercambia σ con τ. Los otros grupos no son conjugados puesto que sus p-subgrupos de Sylow no lo son.

Sea G un subgrupo regular y sea $\pi_2(G) = \mathcal{T}_s \leq \iota(\operatorname{Aut}\mathcal{G}_k)$ para cierto $s \in \mathcal{B}$. Podemos repetir el argumento del lema 5.1.11 para mostrar que G es un conjugado de alguno de los grupos de la tabla (las fórmulas (F_k) y (P_k) se cumplen para $k = 1$).

En otro caso, como en el lema 5.1.26 tenemos que G tiene la forma

$$G = \langle \sigma^{\frac{1}{g-1}}\alpha_1,\ u\alpha_2^i\gamma,\ w\epsilon^c\theta \rangle$$

para $c \neq 0$, $i = 0, 1$ y $\theta \in \{\beta_s, \widetilde{\beta} : 0 \leq s \leq q-1\}$.

- Si $\pi_2(G) = \mathcal{R}_s$, salvo conjugación por una potencia de α_1 podemos suponer que $w \in \langle \tau \rangle$ y que $u \in \langle \tau \rangle$ salvo conjugación por una potencia de γ. Conjugando nuevamente por un automorfismo de la forma $[(0,0), xId]$ podemos suponer que $u = \tau$. Como

$$\beta_s\gamma\beta_s^{-1} = (\gamma)^{g^{1-s}}$$

  la condición (R) implica que los últimos dos generadores de G satisfacen la misma relación. En consecuencia $c = 1 - 2s$ y $w = \tau^{\frac{1-g^{1-s}}{2}}$. Por lo tanto G es un conjugado de $\widetilde{R}_s$. Si $\pi_2(G) = \mathcal{N}$ podemos concluir que G es un conjugado de $\widetilde{N}$ en forma análoga.

- Si $\pi_2(G) = \mathcal{L}$, salvo conjugación por un elemento de la forma

$$h = \left[(0,0), \begin{bmatrix} x^2 & y \\ 0 & x \end{bmatrix}\right]$$

  podemos suponer que $u \in \langle \tau \rangle$. Por (5.19) tenemos que

$$\beta_{2^{-1}}\alpha_2\gamma(\beta_{2^{-1}})^{-1} = \alpha_1^{-g^{2^{-1}}\frac{g^{2^{-1}}-1}{2}}(\alpha_2\gamma)^{g^{2^{-1}}}.$$

  Como en el caso anterior, la condición (R) implica que $w \in \langle \tau \rangle$ y $u = \tau^{\frac{1}{g-1}}$. Finalmente G es un conjugado de $\widetilde{L}_c$ por una potencia adecuada de α_1. $\square$

En las siguientes tablas resumimos el contenido de esta subsección.

$\ker\lambda$	$\mathbb{Z}_p^2 \times \mathbb{Z}_q$	$\mathcal{G}_k,\ k \neq 0, \pm 1, 2$	$\mathcal{G}_2$	$\mathcal{G}_0$	$\mathcal{G}_{-1}$	$\mathcal{G}_1$
1	-	$q+3$	$2q+1$	$q+3$	$\frac{q+3}{2}$	q
p	2	$2(q+1)$	$3q$	$2q$	$q+1$	q
q	2	-	-	-	-	-
pq	-	-	-	2	-	-
p^2	1	$q-1$	$q-1$	$q-1$	$\frac{q-1}{2}$	$q-2$
p^2q	-	-	-	-	-	1

$\ker\lambda$	$\mathbb{Z}_p^2 \times \mathbb{Z}_3$	$\mathcal{G}_0$	$\mathcal{G}_{-1}$	$\mathcal{G}_1$
1	-	6	4	3
p	2	6	5	3
3	2	-	-	-
$3p$	-	2	-	-
p^2	1	2	1	1
$3p^2$	-	-	-	1

Tabla 5.8: Enumeración de brazas torcidas de tipo $\mathcal{G}_1$ con $p = 1 \pmod q$ para el caso $q > 3$ (arriba) y para el caso $q = 3$ (abajo).

5.2. Brazas torcidas de orden p^2q con $p = -1 \pmod q$

En esta sección, suponemos que p y q son primos impares con $p = -1 \pmod q$ (recordemos que estamos omitiendo el caso $q = 2$ y $p^2q = 12$) y que $H(x) = x^2+\xi x+1$ es un polinomio irreducible sobre $\mathbb{Z}_p$ tal que su matriz compañera

$$F = \begin{bmatrix} 0 & -1 \\ 1 & -\xi \end{bmatrix} \tag{5.21}$$

tiene orden q (véase sección 4.3).

Como vimos en la sección 4.3, en estas condiciones tenemos un único grupo no abeliano de orden p^2q:

$$\mathcal{G}_F = \langle \sigma, \tau, \epsilon \,|\, \sigma^p = \tau^p = \epsilon^q = 1,\ \epsilon\sigma\epsilon^{-1} = \tau,\ \epsilon\tau\epsilon^{-1} = \sigma^{-1}\tau^{-\xi} \rangle \cong \mathbb{Z}_p^2 \rtimes_F \mathbb{Z}_q.$$

Un automorfismo de $\mathcal{G}_F$ está determinado por la imagen de los generadores, es decir por la restricción a $\langle \sigma, \tau \rangle$ dada por una matriz y por la imagen de ϵ. De acuerdo con [17, Subsections 4.1, 4.4], la función

$$\phi : \mathbb{Z}_p^2 \rtimes_\rho (N_{GL_2(p)}(F)) \longrightarrow \operatorname{Aut}\mathcal{G}_F, \quad [(n,m), M] \mapsto h_\pm = \begin{cases} h|_{\langle\sigma,\tau\rangle} = M_\pm \\ \epsilon \mapsto \sigma^n\tau^m\epsilon^{\pm 1} \end{cases}$$

donde $\phi([(n,m),M]) = h_+$ si $M \in C_{GL_2(p)}(F)$ y h_- en otro caso, es un isomorfismo de grupos. La forma de $M_\pm = h_\pm|_{\langle\sigma,\tau\rangle}$ es la siguiente:

$$M_+ = \begin{bmatrix} x & -y \\ y & x-\xi y \end{bmatrix}, \quad M_- = \begin{bmatrix} x & y-\xi x \\ y & -x \end{bmatrix} \tag{5.22}$$

donde $x, y \in \mathbb{Z}_p$ y $x^2+y^2-\xi xy \neq 0$. El p-subgrupo de Sylow de $\mathcal{G}_F$ es característico, por lo cual la función

$$\nu : \operatorname{Aut}\mathcal{G}_F \longrightarrow \operatorname{Aut}\mathcal{G}_F/\langle\sigma,\tau\rangle, \quad h_\pm \mapsto \pm 1$$

es un morfismo de grupos. El núcleo de ν es $\operatorname{Aut}\mathcal{G}_F{}^+ = \mathbb{Z}_p^2 \rtimes C_{GL_2(p)}(F)$ y contiene al p-subgrupo de Sylow de $\operatorname{Aut}\mathcal{G}_F$, generado por $\alpha_1 = [(1,0), Id]$ y $\alpha_2 = [(0,1), Id]$, y a los elementos de orden impar de $\operatorname{Aut}\mathcal{G}_F$.

Proposición 5.2.1. *Sea G un subgrupo regular de $\operatorname{Hol}(\mathcal{G}_F)$. Luego $|\pi_2(G)| \neq p, pq$.*

Demostración. Sea G un subgrupo regular de $\operatorname{Hol}(\mathcal{G}_F)$. El grupo $\mathcal{G}_F$ no tiene subgrupos de orden pq y entonces $|\pi_2(G)| \neq p$. El grupo $\mathcal{G}_F$ es el único grupo no abeliano de orden p^2q y no tiene subgrupos normales de orden p. Si $\pi_2(G) = pq$ entonces G tiene un subgrupo normal de orden p y entonces debe ser abeliano. En consecuenca, $\pi_2(G)$ es un subgrupo abeliano de orden pq de $\operatorname{Aut}\mathcal{G}_F$. Por otro lado, $\operatorname{Aut}\mathcal{G}_F$ no tiene subgrupos con esas propiedades, lo que da lugar a una contradicción. □

El subgrupo

$$\mathfrak{H}_F = \langle\sigma,\tau,\alpha_1,\alpha_2\rangle \tag{5.23}$$

es normal en $\operatorname{Hol}(\mathcal{G}_F)$.

Lema 5.2.2. *Las brazas torcidas de tipo $\mathcal{G}_F$ con $|\ker\lambda| = p^2$ son $(B_a,+,\circ)$ donde $(B_a,+) = \mathbb{Z}_p^2 \rtimes_F \mathbb{Z}_q$ y*

$$(B_a,\circ) = \mathbb{Z}_p^2 \rtimes_{F^{\frac{a+1}{a}}} \mathbb{Z}_q \cong \begin{cases} \mathbb{Z}_p^2 \times \mathbb{Z}_q, & \text{si } a = q-1 \\ \mathcal{G}_F, & \text{en otro caso} \end{cases}$$

para $1 \leq a \leq q-1$. En particular son todas bi-brazas.

Demostración. Los grupos

$$G_a = \langle\sigma,\tau,\epsilon^a f\rangle$$

donde $f = [(0,0), F]$ tienen orden p^2q y son regulares. Sea $\mathfrak{H}_F$ el subgrupo de (5.23) y supongamos que G_a y G_b son conjugados entre sí por h, entonces

$$h(\epsilon)^a h f h^{-1}\mathfrak{H}_F = \epsilon^{\pm a} f^{\pm 1}\mathfrak{H}_F = (\epsilon^b f)^n \mathfrak{H}_F$$

para cierto n. Luego $n = \pm 1$ y $a = b$.

Sea G un subgrupo regular de $\operatorname{Hol}(\mathcal{G}_F)$ tal que $|\pi_2(G)| = q$. Salvo conjugación, podemos suponer que $\pi_2(G)$ está generado por f. El núcleo de π_2 es el p-subgrupo de Sylow de $\mathcal{G}_F$ y entonces podemos suponer que

$$G = \langle\sigma,\tau,\epsilon^a f\rangle$$

donde $a \neq 0$. Argumentando igual que en la proposición 5.1.8 podemos exhibir la estructura de la braza torcida asociada al grupo G_a. □

Lema 5.2.3. *Existe una única clase de conjugación de subgrupos regulares G de* $\mathrm{Hol}(\mathcal{G}_F)$ *con* $|\pi_2(G)| = p^2$. *Un representante está dado por*

$$H = \langle \epsilon, u\alpha_1, w\alpha_2 \rangle \cong \mathbb{Z}_p^2 \times \mathbb{Z}_q$$

donde $u = (F-1)^{-1}(\sigma)$ *y* $w = (F-1)^{-1}(\tau)$.

Demostración. El grupo H tiene las propiedades deseadas. Supongamos que G es un subgrupo regular de $\mathrm{Hol}(\mathcal{G}_F)$ con $|\pi_2(G)| = p^2$. Entonces la imagen de π_2 es el p-subgrupo de Sylow normal de $\mathrm{Aut}\,{\mathcal{G}_F}^+$ generado por α_1 y α_2. Salvo conjugación, podemos suponer que el núcleo está generado por ϵ y entonces tenemos que $G = \langle \epsilon, u\alpha_1, w\alpha_2 \rangle$. El núcleo de π_2 es un subgrupo normal de orden q de G y en consecuencia G es abeliano. Luego, por abelianidad, se sigue que $u = (F-1)^{-1}(\sigma)$ y $w = (F-1)^{-1}(\tau)$. □

Observación 5.2.4. Vamos a enunciar algunas propiedades que satisface la transformación lineal definida por la matriz (5.21) y que utilizaremos en lo que sigue.

(i) Sea W un polinomio. Entonces

$$\ker\left(W(F)\right) \neq 0 \text{ si y sólo si } W(F) = 0. \tag{5.24}$$

En efecto $\ker(W(F))$ es un subgrupo F-invariante y entonces es igual a 0 o bien a $\mathbb{Z}_p^2$. Por lo tanto, el álgebra de polinomios generada por F es un cuerpo y, más aún, si W_1 y W_2 son polinomios, entonces $W_1(F) = W_2(F)$ si y sólo si $W_1(F)(x) = W_2(F)(x)$ para cierto $x \neq 0$.

(ii) Sea $n \in \mathbb{N}$. Como

$$\begin{aligned} H(F^n) - H(F) &= F^{2n} - \xi F^n + 1 - (F^2 + \xi F + 1) \\ &= (F^n - F)(F^n + \underbrace{F + \xi}_{=-F^{-1}}) = (F^n - F)(F^n - F^{-1}) \end{aligned}$$

y la matriz F satisface la ecuación $H(F) = F^2 + \xi F + 1 = 0$, tenemos que $H(F^n) = 0$ si y sólo si $n = \pm 1 \pmod q$.

(iii) El automorfismo F actúa en forma irreducible sobre $\mathbb{Z}_p^2$ y entonces

$$\langle x,\, F(x) \rangle = \mathbb{Z}_p^2 \tag{5.25}$$

para todo $x \neq 0$.

Definamos la función Ψ como

$$\Psi : \mathbb{Z}_p^2 \longrightarrow \mathbb{Z}_p, \quad (x, y) \mapsto x^2 + y^2 - x + y - \xi xy.$$

Es fácil ver que Ψ es sobreyectiva.

Lema 5.2.5. *Sea* $v \in \langle \sigma, \tau \rangle$, $\widetilde{v} = F(v) - (1+F)\sigma$ *y* $S_v = \langle \widetilde{v}\alpha_1, v\alpha_2 \rangle \leq \mathrm{Hol}(\mathcal{G}_F)$. *Entonces*

$$|N_{\mathrm{Hol}(\mathcal{G}_F)}(S_v) \cap \mathrm{Aut}\,\mathcal{G}_F| = \begin{cases} 2p^2(p^2-1), & \text{si } v = (\frac{1}{\xi+2}, -\frac{1}{\xi+2}), \\ 2p^2(p-1), & \text{en otro caso.} \end{cases}$$

Más aún, si S_v *y* S_w *son conjugados por un elemento de* $\mathrm{Aut}\,\mathcal{G}_F$ *entonces se cumple que* $\Psi(v) = \Psi(w)$.

Demostración. Sea $h = [(n,m), M_+] \in \mathrm{Aut}\,\mathcal{G}_F$ como definimos en (5.22), es decir que $M_+ \in C_{GL_2(p)}(F)$. Entonces

$$hS_vh^{-1} = \langle M(\widetilde{v})\alpha_1^x\alpha_2^y,\ M(v)\alpha_1^{-y}\alpha_2^{x-\xi y} \rangle.$$

La igualdad $hS_vh^{-1} = S_w$ es equivalente al siguiente sistema lineal de ecuaciones:

$$\begin{cases} M(\tilde{v}) = x\tilde{w} + yw \\ M(v) = -y\tilde{w} + (x - \xi y)w. \end{cases} \tag{5.26}$$

Dados $v = \sigma^n\tau^m$ y $w = \sigma^s\tau^t$, podemos convertir al sistema (5.26) en un sistema lineal en x e y. Este sistema que tiene originalmente 4 ecuaciones en x e y es equivalente al siguiente sistema homogéneo:

$$\begin{bmatrix} m-t & -\xi m + s + n - 1 \\ n-s & -m + \xi s - t - 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = L \begin{bmatrix} x \\ y \end{bmatrix} = 0. \tag{5.27}$$

Si el sistema admite solución no trivial, es decir S_v y S_w son conjguados, entonces $\det(L) = \psi(n,m) - \psi(s,t) = 0$.

Tomando $v = w$, es fácil deducir que si $v = (\frac{1}{\xi+2}, -\frac{1}{\xi+2})$, todo $(x,y) \in \mathbb{Z}_p^2$ es una solución de (5.27), es decir $\mathrm{Aut}\,\mathcal{G}_1$ normaliza S_v. En otro caso, las soluciones de (5.27) están dadas por $y = 0$.

Un argumento similar nos lleva a la misma condición para el caso en que consideramos M_- como en (5.22), con la propiedad $M_-F = F^{-1}M_-$. En ese caso, llegamos a que $S_{(\frac{1}{\xi+2}, -\frac{1}{\xi+2})}$ es normalizado por cualquier $h = [(n,m), M_-]$, caso contrario los coeficientes de M_- satisfacen $x = 0$ e $y \neq 0$. □

Lema 5.2.6. *Un conjunto de representantes de clases de conjugación de subgrupos regulares* G *de* $\mathrm{Hol}(\mathcal{G}_F)$ *tal que* $|\pi_2(G)| = p^2q$ *está dado por*

Grupos	*Parámetros*	*Clase*	#
$G_c = \langle u_c\alpha_1, f(u_c)\alpha_2, \epsilon^c f \rangle$	$1 \leq c \leq q-1,\ c \neq -2$	$\mathcal{G}_F$	$q-2$
$H_a = \langle \widetilde{v_a}\alpha_1, v_a\alpha_2, \epsilon^{-2} f \rangle$	$1 \leq a \leq p-1$	$\mathcal{G}_F$	$p-1$

donde $f = [(0,0), F]$, $u_c = H(F^{c+1})^{-1}(F-1)^{-1}(F^c-1)(F^{c+2}-1)(\sigma)$ *y el conjunto* $\{v_a \in \mathbb{Z}_p^2 : a \in \mathbb{Z}_p\}$ *es un conjunto de representantes de los conjuntos de nivel de* Ψ *con* $\Psi(v_a) = a$ *y* $\widetilde{v_a} = F(v_a) - (1+F)(\sigma)$ *(como definimos en el lema 5.2.5).*

Demostración. Los subgrupos G_c del enunciado son regulares.

De hecho, tenemos $\epsilon^c \in \pi_1(G_c)$ y, de acuerdo con el lema 4.1.4(2), también tenemos que $\langle u_c, f(u_c)\rangle \subseteq \pi_1(G_c)$ y por la observación 5.2.4(iii), $\{u_c, F(u_c)\}$ es una base de $\mathbb{Z}_p^2$. Entonces $|\pi_1(G_c)| > p^2$ y luego $\pi_1(G_c) = \mathcal{G}_F$ (análogamente para H_a).

Si G_c es un conjugado de G_d o de H_a, entonces podemos argumentar como en el lema 5.2.2 y conseguimos que $c = d$ o $c = -2$. Si H_a y H_b son conjugados entonces sus correspondientes p-subgrupos de Sylow también lo son. En consecuencia, por el lema 5.2.5 tenemos $a = \Psi(v_a) = \Psi(v_b) = b$.

El único subgrupo de orden p^2q de $\operatorname{Aut}\mathcal{G}_F$ está generado por los elementos α_1, α_2 y $f = [(0,0), F]$ y es isomorfo a $\mathcal{G}_F$. Entonces la presentación estándar de un subgrupo regular G de $\operatorname{Hol}(\mathcal{G}_F)$ con $|\pi_2(G)| = p^2q$ es

$$G = \langle u\epsilon^a\alpha_1,\ v\epsilon^b\alpha_2,\ w\epsilon^c f\rangle$$

donde $u, v, w \in \langle\sigma, \tau\rangle$. Las condiciones (R) son:

$$(u\epsilon^a\alpha_1)^p = (v\epsilon^b\alpha_2)^p = (w\epsilon^c f)^q = 1 \tag{5.28}$$

$$(w\epsilon^c f)u\epsilon^a\alpha_1(w\epsilon^c f)^{-1} = v\epsilon^b\alpha_2 \tag{5.29}$$

$$(w\epsilon^c f)v\epsilon^b\alpha_2(w\epsilon^c f)^{-1} = (u\epsilon^a\alpha_1)^{-1}(v\epsilon^b\alpha_2)^{-\xi}. \tag{5.30}$$

Por (5.28) obtenemos $a = b = 0$. Si $c = 0$ entonces por el lema 4.1.4(1), se tiene que $\pi_1(G) \subseteq \langle\sigma, \tau\rangle$ y en consecuencia G no sería regular. Podemos suponer entonces que $c \neq 0$ y las ecuaciones (5.29) y (5.30) son equivalentes a

$$\begin{cases} v = F^{c+1}(u) - (F-1)^{-1}(F^c - 1)F(\sigma) \\ h(F^{c+1})(u) = (F-1)^{-1}(F^c - 1)(F^{c+2} - 1)(\sigma). \end{cases} \tag{5.31}$$

De acuerdo con las observaciones 5.2.4(ii) y (i), si $c \neq -2$ entonces $H(F^{c+1})$ es un automorfismo de $\mathbb{Z}_p^2$. Si $c \neq -2$ entonces sustituyendo la segunda ecuación en la primera en el sistema (5.31) y utilizando que $F^2 = -\xi F - 1$ conseguimos que (5.31) es equivalente a

$$\begin{cases} v = F(u) \\ u = h(F^{c+1})^{-1}(F-1)^{-1}(F^c - 1)(F^{c+2} - 1)(\sigma). \end{cases} \tag{5.32}$$

Por lo tanto $u = u_c$ queda unívocamente determinado por c y además

$$G = \langle u_c\alpha_1,\ f(u_c)\alpha_2,\ w\epsilon^c f\rangle$$

donde $c \neq -2$. Si $c + 1 = 0$, la última condición en (5.28) implica que $w = 0$ y entonces $G = G_{-1}$.

En otro caso, veamos que G es un conjugado de G_c por algún elemento de la forma $h = \alpha_1^n\alpha_2^m$ para ciertos n, m. En efecto, h centraliza $\langle u\alpha_1, f(u)\alpha_2\rangle$ y luego $hGh^{-1} = G_c$ si y sólo si el conjugado del último generador pertenece a G_c, es decir

$$\begin{aligned} hw\epsilon^c f h^{-1} &= w'\alpha_1^{n+m}\alpha_2^{-n+(1+\xi)m}\epsilon^c f \\ &= (u_c\alpha_1)^{n+m}(f(u_c)\alpha_2)^{-n+(1+\xi)m}\epsilon^c f \in G_c. \end{aligned} \tag{5.33}$$

La ecuación (5.33) es equivalente a que $w = nx + mF(x)$ donde

$$x = \frac{(F^c-1)(F^{c+1}-1)(F^{c+2}-1)}{(F-1)H(F^{c+1})} \neq 0.$$

De acuerdo con la observación (5.2.4)(iii), $\{x, F(x)\}$ es una base de $\mathbb{Z}_p^2$ y por lo tanto $w \in \langle x, F(x)\rangle$.

Sea $c = -2$. En este caso, la segunda condición de (5.31) es trivial de acuerdo con (5.24) y la primera es equivalente a

$$u = F(v) - (F+1)(\sigma) = \widetilde{v}. \tag{5.34}$$

Si $v = (x, y)$ entonces $\widetilde{v} = (-y-1, x-\xi y-1)$. Como G es regular, entonces u y v son linealmente independientes, es decir

$$\det\begin{bmatrix} v & \widetilde{v}\end{bmatrix} = \det\begin{bmatrix} x & -y-1 \\ y & x-\xi y-1\end{bmatrix} = \Psi(x,y) \neq 0. \tag{5.35}$$

La cantidad de soluciones de la ecuación $\Psi(x, y) = 0$ es $p + 1$, por lo tanto hay $p^2 - p - 1$ elecciones para v.

El p-subgrupo de Sylow de G es el grupo $S_v = \langle \widetilde{v}\alpha_1, v\alpha_2\rangle$. De acuerdo con el lema 5.2.5, si $v = (\frac{1}{\xi+2}, -\frac{1}{\xi+2})$ entonces S_v es normalizado por $\operatorname{Aut}\mathcal{G}_F$, caso contrario su normalizador tiene índice $p + 1$ en $\operatorname{Aut}\mathcal{G}_F$. En consecuencia, hay

$$\frac{p^2-p-2}{p+1} + 1 = \frac{(p-2)(p+1)}{p+1} + 1 = p - 1$$

elecciones para v salvo conjugación y los representantes se pueden elegir para que sean $\{v_a : 0 \neq a \in \mathbb{Z}_p\}$, pues el valor de $\Psi(v)$ es un invariante. Por lo tanto, podemos asumir que G es un conjugado de algún grupo de la forma

$$G = \langle \widetilde{v}_a\alpha_1,\ v_a\alpha_2,\ w\epsilon^{-2}f\rangle$$

para cierto $1 \leq a \leq p-1$. Veamos que G es un conjugado de algún H_a por cierto $h \in \langle \alpha_1, \alpha_2\rangle$. En efecto, esto es equivalente a que

$$hw\epsilon^{-2}fh^{-1} = w\sigma^{m\frac{F^{-2}-1}{F-1}}\tau^{(\xi m-n)\frac{F^{-2}-1}{F-1}}\alpha_1^{n+m}\alpha_2^{m(1+\xi)-n} = (\widetilde{v}_a\alpha_1)^{n+m}(v_a\alpha_2)^{(1+\xi)m-n}.$$

Trabajando con esta condición, resulta ser equivalente a que $w \in \langle x, y\rangle$, donde

$$x = \widetilde{v} - v + z, \quad y = \widetilde{v} + (1+\xi)v + F(z)$$

con $z = (F + \xi - 1)(\sigma)$. Es fácil verificar que

$$\det\begin{bmatrix} x & y\end{bmatrix} = -(\xi+2)\Psi(v_a) \neq 0,$$

es decir que x, y es una base y luego G es un conjugado de H_a. □

Resumimos el contenido de esta sección en la siguiente tabla:

$\lvert\ker\lambda\rvert$	$\mathbb{Z}_p^2 \times \mathbb{Z}_q$	$\mathcal{G}_F$
1	-	$p+q-3$
q	1	-
p^2	1	$q-2$
p^2q	-	1

Tabla 5.9: Enumeración de brazas torcidas de tipo $\mathcal{G}_F$ para $p = -1 \pmod q$.

5.3. Brazas torcidas de orden p^2q con $q = 1 \pmod p$ y $q \neq 1 \pmod{p^2}$

En esta sección asumiremos que p y q son primos tales que $q = 1 \pmod p$ y $q \neq 1 \pmod{p^2}$ (incluyendo el caso $p = 2$ salvo indicación contraria). Sea r un elemento fijo de orden p en $\mathbb{Z}_q^\times$. Como $p^2q \neq 12$, los grupos no abelianos que nos interesan en esta sección son los siguientes:

(i) $\mathbb{Z}_q \rtimes_r \mathbb{Z}_{p^2} = \langle \sigma, \tau \mid \sigma^{p^2} = \tau^q = 1,\ \sigma\tau\sigma^{-1} = \tau^r \rangle$;

(ii) $\mathbb{Z}_p \times (\mathbb{Z}_q \rtimes_r \mathbb{Z}_p) = \langle \sigma, \tau, \epsilon \mid \sigma^p = \tau^p = \epsilon^q = 1,\ [\epsilon, \tau] = [\tau, \sigma] = 1,\ \sigma\epsilon\sigma^{-1} = \epsilon^r \rangle$.

Las tablas 5.10 y 5.11 resumen la enumeración de brazas torcidas de acuerdo a la clase de isomorfismo de sus estructuras aditivas y multiplicativas.

$+\backslash\circ$	$\mathbb{Z}_{p^2q}$	$\mathbb{Z}_q \rtimes_r \mathbb{Z}_{p^2}$	$\mathbb{Z}_p^2 \times \mathbb{Z}_q$	$\mathbb{Z}_p \times (\mathbb{Z}_q \rtimes_r \mathbb{Z}_p)$
$\mathbb{Z}_q \rtimes_r \mathbb{Z}_{p^2}$	$2p$	$2p(p-1)$	-	-
$\mathbb{Z}_p \times (\mathbb{Z}_q \rtimes_r \mathbb{Z}_p)$	-	-	4	$6p-4$

Tabla 5.10: Enumeración de brazas torcidas de orden p^2q con $q = 1 \pmod p$, $q \neq 1 \pmod{p^2}$ y $p > 2$.

$+\backslash\circ$	$\mathbb{Z}_{4q}$	$\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_4$	$\mathbb{Z}_2^2 \times \mathbb{Z}_q$	$\mathbb{Z}_2 \times (\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_2)$
$\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_4$	2	2	2	4
$\mathbb{Z}_2 \times (\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_2)$	2	2	2	4

Tabla 5.11: Enumeración de brazas torcidas de orden $4q$ con $q = 1 \pmod 2$ y $q \neq 1 \pmod 4$. Notemos que en este caso podemos asumir que $r = -1$.

5.3.1. Brazas torcidas de tipo $\mathbb{Z}_q \rtimes_r \mathbb{Z}_{p^2}$

En esta sección notaremos por A al grupo $\mathbb{Z}_q \rtimes_r \mathbb{Z}_{p^2}$. Utilizaremos la siguiente presentación:

$$A = \langle \sigma,\ \tau \mid \sigma^{p^2} = \tau^q = 1,\ \sigma\tau\sigma^{-1} = \tau^r \rangle.$$

De acuerdo con [17, Subsection 4.5], la función

$$\mathbb{Z}_p \times (\mathbb{Z}_q \rtimes \mathbb{Z}_q^\times) \longrightarrow \operatorname{Aut} A, \qquad (k,j,i) \mapsto \varphi_{i,j}^k = \begin{cases} \tau \mapsto \tau^i \\ \sigma \mapsto \tau^j \sigma^{kp+1} \end{cases}$$

es un isomorfismo. En particular, p^2q divide a $|\operatorname{Aut} A| = pq(q-1)$ y entonces tenemos que verificar todos los posibles valores para el orden de la imagen de un subgrupo regular bajo π_2. Notemos que $Z(A) = \langle \sigma^p \rangle$ y luego $\langle \tau, \sigma^p \rangle$ es un subgrupo abeliano característico de A de orden pq.

Las clases de conjugación de los subgrupos de $\operatorname{Aut} A$ están dadas por la tabla 5.12.

Orden	Grupos	Parámetros	Clase
p	$\langle \varphi_{r,0}^k \rangle$	$0 \le k \le p-1$	$\mathbb{Z}_p$
	$\langle \varphi_{1,0}^1 \rangle$	-	
q	$\langle \varphi_{1,1}^0 \rangle$	-	$\mathbb{Z}_q$
p^2	$\langle \varphi_{1,0}^1,\ \varphi_{r,0}^0 \rangle$	-	$\mathbb{Z}_p^2$
pq	$\langle \varphi_{r,0}^k,\ \varphi_{1,1}^0 \rangle$	$0 \le k \le p-1$	$\mathbb{Z}_q \rtimes_r \mathbb{Z}_p$
	$\langle \varphi_{1,0}^1,\ \varphi_{1,1}^0 \rangle$	-	$\mathbb{Z}_{pq}$
p^2q	$\langle \varphi_{1,0}^1,\ \varphi_{r,0}^0,\ \varphi_{1,1}^0 \rangle$	-	$\mathbb{Z}_p \times (\mathbb{Z}_q \rtimes_r \mathbb{Z}_p)$

Tabla 5.12: Clases de conjugación de subgrupos de $\operatorname{Aut} A$.

Lema 5.3.1. *La única braza torcida de tipo A con $|\ker \lambda| = p^2$ es $(B, +, \circ)$ donde*

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} + \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} x_1 + r^{y_1} x_2 \\ y_1 + y_2 \end{pmatrix}, \qquad \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \circ \begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} r^{y_2} x_1 + r^{y_1} x_2 \\ y_1 + y_2 \end{pmatrix}$$

para todos $0 \le x_1, x_2 \le q-1$ y para todos $0 \le y_1, y_2 \le p^2 - 1$. En particular, $(B, \circ) \cong \mathbb{Z}_{p^2q}$.

Demostración. Consideremos el grupo

$$G = \langle \sigma,\ \tau^{\frac{1}{r-1}} \varphi_{1,1}^0 \rangle \cong \mathbb{Z}_{p^2q}.$$

El subconjunto $\pi_1(G)$ contiene a $\langle \sigma \rangle$ y a $\tau^{\frac{1}{r-1}}$ y por lo tanto $|\pi_1(G)| > p^2$. Como además divide a p^2q, tenemos que $\pi_1(G) = A$ y de acuerdo con el lema 4.1.3 tenemos que G es regular.

Sea G un subgrupo regular de $\operatorname{Hol}(A)$ con $|\pi_2(G)| = q$. Por la tabla 5.12, tenemos que $\pi_2(G) = \langle \varphi_{1,1}^0 \rangle$, que resulta ser un subgrupo normal de $\operatorname{Aut} A$. Los subgrupos de orden p^2 de A son todos conjugados de $\langle \sigma \rangle$, por lo cual G tiene la siguiente presentación estándar:

$$G = \langle \sigma,\ \tau^a \sigma^b \varphi_{1,1}^0 \rangle = \langle \sigma,\ \tau^a \varphi_{1,1}^0 \rangle.$$

Por la condición (K), tenemos que $a = \frac{1}{r-1}$. La fórmula del enunciado se sigue por el mismo argumento del lema 5.1.4. □

Vamos a considerar el grupo $\mathfrak{G}_1 = \langle \sigma^p,\ \tau,\ \varphi^0_{1,1} \rangle \trianglelefteq \mathrm{Hol}(A)$ para el cual se cumple que $\mathrm{Hol}(A)/\mathfrak{G}_1 \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_q^\times$.

Lema 5.3.2. *Un conjunto de representantes de clases de conjugación de subgrupos regulares G de* $\mathrm{Hol}(A)$ *con* $|\pi_2(G)| = p$ *está dado por*

$\pi_2(G)$	*Grupos*	*Parámetros*	*Clase*	#
$\langle \varphi^1_{1,0} \rangle$	$G_a = \langle \tau,\ \sigma^p,\ \sigma^a\varphi^1_{1,0} \rangle$	$1 \leq a \leq p-1$,	A, *si* $p > 2$ $\mathbb{Z}_2 \times (\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_2)$, *si* $p = 2$	$p-1$
$\langle \varphi^k_{r,0} \rangle$	$H_{a,k} = \langle \tau,\ \sigma^p,\ \sigma^a\varphi^k_{r,0} \rangle$	$1 \leq a \leq p-1$, $0 \leq k \leq p-1$	$p > 2 : \begin{cases} \mathbb{Z}_{p^2q} & si\ a = p-1 \\ A & en\ otro\ caso \end{cases}$ $p = 2 : \begin{cases} \mathbb{Z}_{4p} & si\ k = 0 \\ \mathbb{Z}_2^2 \times \mathbb{Z}_p & si\ k = 1 \end{cases}$	$p(p-1)$

Demostración. Los grupos G de orden p^2q en la tabla tienen la forma general:

$$\langle \tau,\ \sigma^p,\ \sigma^a\theta \rangle$$

donde $1 \leq a \leq p-1$ y $\theta \in \{\varphi^1_{1,0}, \varphi^k_{r,0}\}$. Luego, $\langle \tau, \sigma^p \rangle \subseteq \pi_1(G)$ y $\sigma^a \in \pi_1(G)$. Por lo tanto $|\pi_1(G)| > pq$ y además divide a p^2q. Entonces, $\pi_1(G) = A$ y de acuerdo con el lema 4.1.3 tenemos que G es regular.

Si G_a y G_b son conjugados entre sí entonces sus imágenes por el epimorfismo canónico al cociente $\mathrm{Hol}(A)/\mathfrak{G}_1$ son iguales, es decir $\langle \sigma^a\varphi^1_{1,0} \rangle = \langle \sigma^b\varphi^1_{1,0} \rangle$ y por lo tanto $a = b$ (la misma idea aplica para los grupos $H_{a,k}$). Más aún, G_a y $H_{b,k}$ no son conjugados puesto que sus imágenes por π_2 no lo son.

El único subgrupo de orden pq en A es $\langle \tau, \sigma^p \rangle$. Si G es un subgrupo regular de $\mathrm{Hol}(A)$, debemos considerar dos casos de acuerdo con la tabla 5.12. Si $\pi_2(G) = \langle \varphi^1_{1,0} \rangle$ entonces G tiene la siguiente presentación estándar:

$$G = \langle \tau,\ \sigma^p,\ \tau^b\sigma^a\varphi^1_{1,0} \rangle = \langle \tau,\ \sigma^p,\ \sigma^a\varphi^1_{1,0} \rangle$$

donde $1 \leq a \leq p-1$, es decir $G = G_a$.

Si $\pi_2(G) = \langle \varphi^k_{r,0} \rangle$ para $0 \leq k \leq p-1$, una presentación estándar de G es

$$G = \langle \tau,\ \sigma^p,\ \sigma^a\varphi^k_{r,0} \rangle$$

con $1 \leq a \leq p-1$, es decir $G = H_{a,k}$. □

Lema 5.3.3. *Un conjunto de representantes de las clases de conjugación de subgrupos regulares G de* $\mathrm{Hol}(A)$ *con* $|\pi_2(G)| = pq$ *es*

$\pi_2(G)$	*Grupos*	*Parámetros*	*Clase*	#
$\langle \varphi^1_{1,0},\ \varphi^0_{1,1} \rangle$	$G_a = \langle \sigma^p,\ \sigma^a\varphi^1_{1,0},\ \tau^{\frac{1}{r-1}}\varphi^0_{1,1} \rangle$	$1 \leq a \leq p-1$	$p > 2 : \mathbb{Z}_{p^2q}$ $p = 2 : \mathbb{Z}_2 \times (\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_2)$	$p-1$
$\langle \varphi^k_{r,0},\ \varphi^0_{1,1} \rangle$	$H_{a,k} = \langle \sigma^p,\ \sigma^a\varphi^k_{r,0},\ \tau^{\frac{1}{r-1}}\varphi^0_{1,1} \rangle$	$1 \leq a \leq p-1$ $0 \leq k \leq p-1$	$p > 2 : A$ $p = 2 : \begin{cases} \mathbb{Z}_{4q} & si\ k = 0 \\ \mathbb{Z}_2^2 \times \mathbb{Z}_q & si\ k = 1 \end{cases}$	$p(p-1)$

Demostración. El mismo argumento del lema 5.3.2 muestra que los grupos del enunciado son regulares y que no son conjugados entre sí.

Sea G un subgrupo regular de $\mathrm{Hol}(A)$ tal que $|\pi_2(G)| = pq$. De acuerdo con la tabla 5.12 tenemos dos casos y en ambos la imagen de π_2 es normal. Salvo conjugación, el único subgrupo de orden p de A es $\langle\sigma^p\rangle$ y entonces $\ker\pi_2 = \langle\sigma^p\rangle$. Si $\pi_2(G) = \langle\varphi^1_{1,0},\, \varphi^0_{1,1}\rangle$ entonces

$$G = \langle\sigma^p,\ \tau^b\sigma^a\varphi^1_{1,0},\ \tau^c\sigma^d\varphi^0_{1,1}\rangle.$$

Por las condiciones (R) tenemos que:

- el tercer generador tiene orden q módulo $\langle\sigma^p\rangle$ y se sigue que $d = 0 \pmod p$;
- los últimos dos generadores conmutan módulo $\langle\sigma^p\rangle$ y por lo tanto $c = \frac{1}{r-1}$.

Si $a = 0 \pmod p$ entonces por el lema 4.1.4(1) se tiene que $\pi_1(G) \subseteq \langle\sigma^p, \tau\rangle$, lo cual es una contradicción por regularidad. Por lo tanto, podemos suponer que $1 \leq a \leq p-1$ y entonces

$$G = \langle\sigma^p,\ \tau^b\sigma^a\varphi^1_{1,0},\ \tau^{\frac{1}{r-1}}\varphi^0_{1,1}\rangle.$$

Ahora, el grupo G es un conjugado de G_a por $h = \varphi^0_{1,n}$ donde $n = b\frac{1-r}{r^a-1}$.

Si $\pi_2(G) = \langle\varphi^k_{r,0},\, \varphi^0_{1,1}\rangle$ entonces, por los mismos cálculos del caso anterior, la presentación estándar para G es

$$G = \langle\sigma^p,\ \tau^b\sigma^a\varphi^k_{r,0},\ \tau^{\frac{1}{r-1}}\varphi^0_{1,1}\rangle.$$

Por el mismo argumento, podemos suponer que $1 \leq a \leq p-1$. Si $a = p-1$, a partir de $(\tau^b\sigma^{p-1}\varphi^k_{r,0})^p = \tau^{bp}(\sigma^{p-1}\varphi^k_{r,0})^p \in \langle\sigma^p\rangle$ se sigue que $b = 0$. En otro caso, G es un conjugado de $H_{a,k}$ por medio de alguna potencia de $\varphi^0_{1,1}$. Para ver esto, notemos que $\varphi^0_{1,n} = (\varphi^0_{1,1})^n$ centraliza al primer y al tercer generador de G y que se cumple que

$$\begin{aligned}(\varphi^0_{1,n})(\tau^b\sigma^a\varphi^k_{r,0})(\varphi^0_{1,n})^{-1} &= \tau^{b+n\frac{r^a-1}{r-1}}\sigma^a(\varphi^0_{1,1})^{(1-r)n}\varphi^k_{r,0}\\ &= \tau^{b+n\frac{r^{a+1}-1}{r-1}}(\tau^{\frac{1}{r-1}}\varphi^0_{1,1})^{(1-r)n}\sigma^a\varphi^k_{r,0}.\end{aligned}$$

Luego, $n = b\frac{1-r}{r^{a+1}-1}$ nos servirá. □

Proposición 5.3.4. *Sean $p > 2$ y G un subgrupo regular de* $\mathrm{Hol}(A)$. *Entonces* $|\pi_2(G)| \notin \{p^2, p^2q\}$.

Demostración. Si $p > 2$ entonces

$$(\sigma^a\varphi^1_{1,0})^n = \sigma^{a\left(p\frac{n(n-1)}{2}+n\right)}\left(\varphi^1_{1,0}\right)^n \tag{5.36}$$

para todo $n \in \mathbb{N}$.

Sea G un subgrupo de $\mathrm{Hol}(A)$ de orden p^2q. Si $|\pi_2(G)| = p^2$ entonces de acuerdo con la tabla 5.12 y el hecho de que el núcleo de π_2 es el q-subgrupo de Sylow normal de A, tenemos la siguiente presentación estándar para G:

$$G = \langle \tau,\ \tau^b\sigma^a\varphi^1_{1,0},\ \tau^d\sigma^c\varphi^0_{r,0}\rangle = \langle \tau,\ \sigma^a\varphi^1_{1,0},\ \sigma^c\varphi^0_{r,0}\rangle.$$

Por la condición (R), $(\sigma^a\varphi^1_{1,0})^p = (\sigma^c\varphi^0_{r,0})^p \in \langle\tau\rangle$. Usando la ecuación (5.36) tenemos que $a = c = 0 \pmod p$.

Supongamos que $|\pi_2(G)| = p^2q$. De acuerdo con la tabla 5.12, G tiene la siguiente presentación estándar:

$$G = \langle \tau^a\sigma^b\varphi^1_{1,0},\ \tau^c\sigma^d\varphi^0_{r,0},\ \tau^e\sigma^f\varphi^0_{1,1}\rangle$$

donde los primeros dos generadores tiene orden p y el tercero tiene orden q. Luego, $f = 0$ y $b = d = 0 \pmod p$ para lo cual estamos utilizando la fórmula (5.36) nuevamente. El grupo $\langle\sigma^p, \tau\rangle$ es característico en A.

Por lo tanto, en ambos casos, de acuerdo con el lema 4.1.4(1) tenemos que $\pi_1(G) \subseteq \langle\sigma^p, \tau\rangle$ y entonces G no es regular. □

El último resultado es bastante diferente cuando consideramos el caso $p = 2$. Podemos verlo en los siguientes lemas.

Lema 5.3.5. *Sea $p = 2$. Existe una única clase de conjugación de subgrupos regulares de* $\mathrm{Hol}(A)$ *con $|\pi_2(G)| = 4$. Un representante está dado por*

$$H = \langle \tau,\ \sigma\varphi^1_{1,0},\ \sigma^2\varphi^0_{-1,0}\rangle \cong \mathbb{Z}_2 \times (\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_2).$$

Demostración. Para el grupo H, tenemos que $\{\tau^n, \tau^n\sigma : 0 \leq n \leq q-1\} \subseteq \pi_1(H)$ y $\sigma^2 \in \pi_1(H)$. Luego, $|\pi_1(H)| > 2q$ y debe dividir a $4q$. Entonces, H es regular por el lema 4.1.3.

Sea G un subgrupo regular con $|\pi_2(G)| = 4$. De acuerdo con la tabla 5.12, tenemos que G tiene la siguiente presentación estándar:

$$G = \langle \tau,\ \sigma^a\varphi^1_{1,0},\ \sigma^b\varphi^0_{-1,0}\rangle$$

donde $1 \leq a, b \leq 3$. Por la condición (R) tenemos que $(\sigma^b\varphi^0_{-1,0})^2 = \sigma^{2b} \in \langle\tau\rangle$, por lo tanto $b = 2$. En consecuencia, $a = 1$ o $a = 3$. Si $a = 1$, tenemos que $G = H$ y si $a = 3$, el grupo G es un conjugado de H por $\varphi^1_{1,0}$. □

Lema 5.3.6. *Sea $p = 2$. Existe una única clase de conjugación de subgrupos regulares con $|\pi_2(G)| = 4q$. Un representante está dado por*

$$H = \langle \sigma\varphi^1_{1,0},\ \sigma^2\varphi^0_{-1,0},\ \tau^{-\frac{1}{2}}\varphi^0_{1,1}\rangle \cong \mathbb{Z}_2 \times (\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_2).$$

Demostración. Análogamente al lema 5.3.5, se puede verificar inmediatamente que el grupo del enunciado es un subgrupo regular de $\mathrm{Hol}(A)$. Un subgrupo regular con $|\pi_2(G)| = 4q$ tiene la siguiente presentación estándar:

$$G = \langle \tau^a\sigma^b\varphi^1_{1,0},\ \tau^c\sigma^d\varphi^0_{-1,0},\ \tau^e\sigma^f\varphi^0_{1,1}\rangle.$$

Por la condición (R) tenemos que $(\tau^a\sigma^b\varphi^1_{1,0})^2 = (\tau^c\sigma^d\varphi^0_{-1,0})^2 = (\tau^e\sigma^f\varphi^0_{1,1})^q = 1$ y entonces $b \in \{1,3\}$, $d \in \{0,2\}$ y $f = 0$. Como $\varphi^1_{1,0}$ es un elemento central en $\pi_2(G)$, nuevamente por la condición (R), tenemos que $\tau^a\sigma^b\varphi^1_{1,0}$ es central en G, por lo tanto $a = c$ y $e = -\frac{1}{2}$ y luego

$$G = \langle \tau^a\sigma^b\varphi^1_{1,0},\ \tau^c\sigma^d\varphi^0_{-1,0},\ \tau^{-\frac{1}{2}}\varphi^0_{1,1}\rangle$$

para cierto $1 \leq a \leq q-1$ y las condiciones sobre b y d de antes. Podemos suponer que $b = 1$, en otro caso conjugamos por $\varphi^1_{1,0}$. Si conjugamos por $\varphi^0_{1,-a}$, obtenemos

$$G = \langle \sigma\varphi^1_{1,0},\ \sigma^d\varphi^0_{-1,0},\ \tau^{-\frac{1}{2}}\varphi^0_{1,1}\rangle.$$

Por último, por regularidad se sigue que $d \neq 0$, y en consecuencia $d = 2$ y conseguimos el grupo H. □

Resumimos el contenido de esta subsección en las siguientes tablas:

$\lvert\ker\lambda\rvert$	$\mathbb{Z}_{p^2q}$	$\mathbb{Z}_q \rtimes_r \mathbb{Z}_{p^2}$
p	$p-1$	$p(p-1)$
pq	p	p^2-p-1
p^2	1	-
p^2q	-	1

$\lvert\ker\lambda\rvert$	$\mathbb{Z}_{4q}$	$\mathbb{Z}_2^2 \times \mathbb{Z}_q$	$\mathbb{Z}_2 \times (\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_2)$	$\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_4$
1	-	-	1	-
2	-	1	1	1
4	1	-	-	-
q	-	-	1	-
$2q$	1	1	1	-
$4q$	-	-	-	1

Tabla 5.13: Enumeración de brazas torcidas de tipo A para $q = 1 \pmod p$, $q \neq 1 \pmod{p^2}$ y $p > 2$ (arriba) $q = 1 \pmod p$, $q \neq 1 \pmod{p^2}$ y $p = 2$ (abajo).

5.3.2. Brazas torcidas de tipo $\mathbb{Z}_p \times (\mathbb{Z}_q \rtimes_r \mathbb{Z}_p)$

En esta sección notaremos por A al grupo $\mathbb{Z}_p \times (\mathbb{Z}_q \rtimes_r \mathbb{Z}_p)$. Una presentación de este grupo es

$$A = \langle \sigma, \tau, \epsilon \,|\, \sigma^p = \tau^p = \epsilon^q = 1,\ [\epsilon,\tau] = [\tau,\sigma] = 1,\ \sigma\epsilon\sigma^{-1} = \epsilon^r\rangle.$$

De acuerdo con [17, Subsection 4.6] la función

$$\phi : (\mathbb{Z}_p \rtimes \mathbb{Z}_p^\times) \times (\mathbb{Z}_q \rtimes \mathbb{Z}_q^\times) \longrightarrow \operatorname{Aut} A, \quad [(l,i),(s,j)] \mapsto \alpha_{l,i}\beta_{s,j}$$

donde

$$\alpha_{l,i} = \begin{cases} \epsilon \mapsto \epsilon \\ \tau \mapsto \tau^i \\ \sigma \mapsto \tau^l\sigma \end{cases} \quad \text{y} \quad \beta_{s,j} = \begin{cases} \epsilon \mapsto \epsilon^j \\ \tau \mapsto \tau \\ \sigma \mapsto \epsilon^s\sigma \end{cases}$$

es un isomorfismo de grupos. En particular, notemos que $\alpha_{l,i}$ y $\beta_{s,j}$ conmutan. En particular, p^2q divide a $|\operatorname{Aut} A| = pq(p-1)(q-1)$ y por lo tanto debemos considerar todos los valores posibles para el orden de la imagen de un subgrupo regular por π_2. Las clases de conjugación de subgrupos de $\operatorname{Aut} A$ aparecen en la tabla 5.14.

Orden	Grupos	Clase
p	$\langle \alpha_{1,1} \rangle$	$\mathbb{Z}_p$
	$\langle \beta_{0,r} \rangle$	
	$\langle \alpha_{1,1}\beta_{0,r} \rangle$	
q	$\langle \beta_{1,1} \rangle$	$\mathbb{Z}_q$
pq	$\langle \alpha_{1,1},\ \beta_{1,1} \rangle$	$\mathbb{Z}_{pq}$
	$\langle \beta_{0,r},\ \beta_{1,1} \rangle$	$\mathbb{Z}_q \rtimes_r \mathbb{Z}_p$
	$\langle \alpha_{1,1}\beta_{0,r},\ \beta_{1,1} \rangle$	$\mathbb{Z}_q \rtimes_r \mathbb{Z}_p$
p^2	$\langle \alpha_{1,1},\ \beta_{0,r} \rangle$	$\mathbb{Z}_p^2$
p^2q	$\langle \alpha_{1,1},\ \beta_{1,1},\ \beta_{0,r} \rangle$	A

Tabla 5.14: Clases de conjugación de subgrupos de $\operatorname{Aut} A$.

El procedimiento para verificar la regularidad de un subgrupos ya lo realizamos en suficientes ocasiones por lo que omitiremos esa parte en lo que resta de la sección 5.3.

Proposición 5.3.7. *La única braza torcida de tipo A con $|\ker \lambda| = p^2$ está dada por $B = B_1 \times B_2$, donde B_1 es la braza torcida trivial de orden p y B_2 es la única braza torcida de tipo no abeliano de orden pq con $|\ker \lambda_{B_2}| = p$. En particular, $(B, \circ) \cong \mathbb{Z}_p^2 \times \mathbb{Z}_q$.*

Demostración. El único subgrupo de orden q de $\operatorname{Aut} A$ está generado por $\beta_{1,1}$ y el núcleo es un p-subgrupo de Sylow de A que podemos tomar como $\langle \sigma, \tau \rangle$ salvo conjugación. Por lo tanto $I = \langle \tau \rangle_+ \leq \ker \lambda \cap \operatorname{Fix}(B) \cap Z(B, +)$ y entonces I es un ideal de B contenido en $Z(B, \circ)$. El subgrupo $J = \langle \epsilon, \sigma \rangle_+ \trianglelefteq (B, +)$ es un ideal a izquierda y como $\tau \in Z(B, \circ)$ entonces J es un ideal de B. Luego, $B = I + J$ y $I \cap J = 0$ y entonces B es un producto directo de la braza torcida trivial de orden p y una braza torcida B_2 de orden pq con $|\ker \lambda_{B_2}| = p$. De acuerdo con el teorema 3.3.6, existe una única braza torcida con esas condiciones y cumple que $(B_2, \circ) \cong \mathbb{Z}_{pq}$. $\square$

En lo que sigue vamos a considerar al subgrupo $\mathfrak{G}_2 = \langle \epsilon, \tau, \alpha_{1,1}, \beta_{1,1} \rangle \trianglelefteq \operatorname{Hol}(A)$. Este subgrupo cumple que $\operatorname{Hol}(A)/\mathfrak{G}_2 \cong \mathbb{Z}_p \times \mathbb{Z}_p^\times \times \mathbb{Z}_q^\times$.

Lema 5.3.8. *Un conjunto de representantes de clases de conjugación de subgrupos regulares G de* $\mathrm{Hol}(A)$ *con* $|\pi_2(G)| = p$ *es*

$\pi_2(G)$	*Grupos*	*Parámetros*	*Clase*	$\#$
$\langle \alpha_{1,1} \rangle$	$K = \langle \epsilon,\ \tau,\ \sigma\alpha_{1,1} \rangle$	-	$p > 2 : A$ $p = 2 : \mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_4$	1
$\langle \beta_{0,r} \rangle$	$L = \langle \epsilon,\ \sigma,\ \tau\beta_{0,r} \rangle$	-	A	1
	$G_c = \langle \epsilon,\ \tau,\ \sigma^c\beta_{0,r} \rangle$	$1 \leq c \leq p-1$	$p > 2 : \begin{cases} \mathbb{Z}_p^2 \times \mathbb{Z}_q & si\ c = -1 \\ A & si\ c \neq -1 \end{cases}$ $p = 2 : \mathbb{Z}_2^2 \times \mathbb{Z}_q$	$p-1$
$\langle \alpha_{1,1}\beta_{0,r} \rangle$	$H_c = \langle \epsilon,\ \tau,\ \sigma^c\alpha_{1,1}\beta_{0,r} \rangle$	$1 \leq c \leq p-1$	$p > 2 : \begin{cases} \mathbb{Z}_p^2 \times \mathbb{Z}_q & si\ c = -1 \\ A & si\ c \neq -1 \end{cases}$ $p = 2 : \mathbb{Z}_{4q}$	$p-1$

Demostración. Los grupos K, L, G_c y H_c no son conjugados entre sí ya que sus imágenes por π_2 o bien sus núcleos no lo son. Si G_c y G_d (resp. H_c y H_d) son conjugados, entonces sus imágenes en el cociente $\mathrm{Hol}(A)/\mathfrak{G}_2$ coinciden, es decir $\langle \sigma^c\beta_{0,r}\mathfrak{G}_2 \rangle = \langle \sigma^d\beta_{0,r}\mathfrak{G}_2 \rangle$. Luego, $c = d$.

Sea G un subgrupo regular de $\mathrm{Hol}(A)$ tal que $|\pi_2(G)| = p$. De acuerdo con la tabla 5.14 debemos discutir tres casos. Supongamos que $\pi_2(G) = \langle \alpha_{1,1} \rangle$. Entonces el núcleo tiene orden pq y entonces G tiene la forma

$$G = \langle \epsilon,\ \sigma^n\tau^m,\ \sigma^a\tau^b\alpha_{1,1} \rangle.$$

Por la condición (K) tenemos que $n = 0$. Por lo tanto, podemos suponer que $b = 0$ y $G = \langle \epsilon,\ \tau,\ \sigma^a\alpha_{1,1} \rangle$. Por regularidad, $a \neq 0$ y entonces G es un conjugado de K por $\alpha_{0,a}$.

Supongamos que $\pi_2(G) = \langle \beta_{0,r} \rangle$. Entonces G tiene la siguiente presentación estándar:

$$G = \langle \epsilon,\ \sigma^n\tau^m,\ \sigma^a\tau^b\beta_{0,r} \rangle.$$

Si $n = 0$ entonces $G = G_a$. Si $n \neq 0$, podemos suponer que $m = 0$, en caso contrario, conjugamos por $\alpha_{1,1}^{-\frac{m}{n}}$. Por lo tanto, podemos suponer que $a = 0$ y $n = 1$. Por regularidad, $b \neq 0$ y entonces G es un conjugado de L por $\alpha_{0,b^{-1}}$.

Por último, supongamos que $\pi_2(G) = \langle \alpha_{1,1}\beta_{0,r} \rangle$. Entonces

$$G = \langle \epsilon,\ \sigma^n\tau^m,\ \sigma^a\tau^b\alpha_{1,1}\beta_{0,r} \rangle.$$

La condición (K) implica que $n = 0$ y entonces $G = \langle \epsilon,\ \tau,\ \sigma^a\alpha_{1,1}\beta_{0,r} \rangle = H_a$.

Notemos que para el caso $p = 2$, los grupos K y H_1 (que es el único H_c) tienen elementos de orden 4 pues $(\sigma\alpha_{1,1})^2 = (\sigma\alpha_{1,1}\beta_{0,r})^2 = \tau$. Para $p > 2$, no hay elementos de orden p^2 y entonces tenemos diferentes clases de isomorfismo en la tabla. □

Lema 5.3.9. *Un conjunto de representantes de clases de conjugación de subgrupos regulares G de* $\mathrm{Hol}(A)$ *con* $|\pi_2(G)| = pq$ *está dado por la siguiente tabla*

$\pi_2(G)$	*Grupos*	*Parámetros*	*Clase*	$\#$
$\langle \alpha_{1,1}, \beta_{1,1} \rangle$	$K_1 = \langle \tau,\ \sigma\alpha_{1,1},\ \epsilon^{\frac{1}{r-1}}\beta_{1,1} \rangle$	-	$p > 2 : \mathbb{Z}_p^2 \times \mathbb{Z}_q$ $p = 2 : \mathbb{Z}_{4q}$	1
$\langle \beta_{1,1}, \beta_{0,r} \rangle$	$K_2 = \langle \sigma,\ \tau\beta_{0,r},\ \epsilon^{\frac{1}{r-1}}\beta_{1,1} \rangle$	-	A	1
	$G_a = \langle \tau,\ \sigma^a\beta_{0,r},\ \epsilon^{\frac{1}{r-1}}\beta_{1,1} \rangle$	$1 \leq a \leq p-1$	A	$p-1$
$\langle \beta_{1,1}, \alpha_{1,1}\beta_{0,r} \rangle$	$H_a = \langle \tau,\ \sigma^a\alpha_{1,1}\beta_{0,r},\ \epsilon^{\frac{1}{r-1}}\beta_{1,1} \rangle$	$1 \leq a \leq p-1$	$p > 2 : A$ $p = 2 : \mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_4$	$p-1$

Demostración. Por el mismo argumento del lema 5.3.8 podemos ver que los grupos de la tabla no son conjugados entre sí. Sea G un subgrupo regular de $\mathrm{Hol}(A)$ con $|\pi_2(G)| = pq$. De acuerdo con la tabla 5.14 debemos considerar tres casos. En todos ellos, actuando por el normalizador de $\pi_2(G)$ si fuera necesario, podemos suponer que $\ker \pi_2|_G$ está generado por τ o por σ.

Sea $\pi_2(G) = \langle \alpha_{1,1},\ \beta_{1,1} \rangle$. Por la condición (K) tenemos que $\ker \pi_2|_G = \langle \tau \rangle$. Luego,

$$G = \langle \tau,\ \epsilon^a\sigma^b\alpha_{1,1},\ \epsilon^c\sigma^d\beta_{1,1} \rangle.$$

La condición (R) implica que $d = 0$ y $c = \frac{1}{r-1}$. Si $b = 0$ entonces, por el lema 4.1.4(1), $\pi_1(G) \subseteq \langle \epsilon, \tau \rangle$, una contradicción puesto que G es regular. Luego $b \neq 0$ y en consecuencia G es un conjugado de K_1 por $\alpha_{0,b}\beta_{1,1}^n$ donde $n = a\frac{1-r}{r^b-1}$.

Sea $\pi_2(G) = \langle \beta_{0,r},\ \beta_{1,1} \rangle$. Si $\ker \pi_2|_G = \langle \sigma \rangle$ entonces

$$G = \langle \sigma,\ \epsilon^a\tau^b\beta_{0,r},\ \epsilon^c\tau^d\beta_{1,1} \rangle.$$

De acuerdo con la condición (K) tenemos $c = \frac{1}{r-1}$ y $a = 0$ (luego, $b \neq 0$ por regularidad) y por (R) tenemos $d = 0$. Luego G es un conjugado de K_2 por $\alpha_{0,b^{-1}}$.

Si $\ker \pi_2|_G$ está generado por τ entonces

$$G = \langle \tau,\ \epsilon^a\sigma^b\beta_{0,r},\ \epsilon^c\sigma^d\beta_{1,1} \rangle.$$

De las condiciones (R) tenemos que $d = 0$ y $c = \frac{1}{r-1}$. Entonces, $b \neq 0$ pues en caso contrario tendríamos $\pi_1(G) \subseteq \langle \tau, \epsilon \rangle$. Si $b + 1 = 0$ entonces ϵ conmuta con $\sigma^b\beta_{0,r}$ y como $(\epsilon^a\sigma^b\beta_{0,r})^p \in \langle \tau \rangle$ tenemos $a = 0$, y en consecuencia $G = G_{-1}$. En otro caso, G es un conjugado de G_b por $\beta_{1,1}^n$ donde $n = a\frac{1-r}{r^{b+1}-1}$.

Sea $\pi_2(G) = \langle \alpha_{1,1}\beta_{0,r},\ \beta_{1,1} \rangle$. La condición (K) implica que $\ker \pi_2|_G = \langle \tau \rangle$. Entonces

$$G = \langle \tau,\ \epsilon^a\sigma^b\alpha_{1,1}\beta_{0,r},\ \epsilon^c\sigma^d\beta_{1,1} \rangle.$$

Las condiciones (R) nos dicen que $d = 0$ y $c = \frac{1}{r-1}$. Además, tenemos que $b \neq 0$ como antes. De la misma forma, si $b + 1 = 0$ entonces $a = 0$ y luego $G = H_{-1}$. Si no, G es un conjugado de H_b por $\beta_{1,1}^n$ donde $n = a\frac{1-r}{r^{b+1}-1}$.

En forma análoga al lema 5.3.8, notemos que para el caso $p = 2$, los grupos K_1 y H_1 (que resulta ser el único H_c) tienen elementos de orden 4 puesto que $(\sigma\alpha_{1,1})^2 = (\sigma\alpha_{1,1}\beta_{0,r})^2 = \tau$. Luego, las clases de isomorfismo de estos grupos son diferentes a las del caso $p > 2$ de la tabla del enunciado. □

Al igual que en la subsección anterior, para los siguientes resultados tendremos diferentes consecuencias según si $p = 2$ o $p > 2$. Recordemos que si $p = 2$ podemos suponer que $r = -1$.

Proposición 5.3.10. *Sea $p = 2$. Si G es un subgrupo regular de* $\mathrm{Hol}(A)$ *entonces* $|\pi_2(G)| \notin \{4, 4q\}$.

Demostración. Supongamos que G es un subgrupo de orden p^2q de $\mathrm{Hol}(A)$ tal que $|\pi_2(G)| = 4$. Por la tabla 5.14 y el hecho de que A tiene un único q-subgrupo de Sylow, tenemos que G tiene la siguiente presentación estándar:

$$G = \langle \epsilon,\ \sigma^a\tau^b\alpha_{1,1},\ \sigma^c\tau^d\beta_{0,-1}\rangle$$

para ciertos $0 \leq a, b, c, d \leq 1$. Por la condición (R), como $(\sigma^a\tau^b\alpha_{1,1})^2 \in \langle\epsilon\rangle$ tenemos que $a = 0$. Además, tenemos que el segundo generador debe conmutar con el tercero módulo el núcleo, luego $c = 0$.

Ahora, supongamos que $|\pi_2(G)| = 4q$, luego G tiene la siguiente presentación estándar:

$$G = \langle \epsilon^a u\alpha_{1,1},\ \epsilon^b v\beta_{0,-1},\ \epsilon^c w\beta_{1,1}\rangle$$

donde $u, v, w \in \langle\sigma, \tau\rangle$. Por la condición (K), el primer generador tiene orden 2 y tenemos que $u \in \langle\tau\rangle$. Como $\alpha_{1,1}\beta_{0,-1} = \beta_{0,-1}\alpha_{1,1}$, la condición (R) nos lleva a que $v \in \langle\tau\rangle$. Por el mismo motivo, $\alpha_{1,1}\beta_{1,1} = \beta_{1,1}\alpha_{1,1}$ implica que $w \in \langle\tau\rangle$.

En consecuencia, en ambos casos $\pi_1(G) \subseteq \langle\tau, \epsilon\rangle$ por el lema 4.1.4(1) y entonces G no es regular. □

Los dos lemas siguientes sólo funcionan para primos impares. En las demostraciones utilizaremos que si $p > 2$ entonces

$$(\sigma^a\alpha_{1,1})^n = \tau^{a\frac{n(n-1)}{2}}\sigma^{na}\alpha_{1,1}^n \tag{5.37}$$

para todo $n \in \mathbb{N}$.

Lema 5.3.11. *Sea $p > 2$. Un conjunto de representantes de clases de conjugación de subgrupos regulares G de* $\mathrm{Hol}(A)$ *con $|\pi_2(G)| = p^2$ es*

$$G_a = \langle \epsilon,\ \sigma^a\alpha_{1,1},\ \tau\beta_{0,r}\rangle \cong A$$

para $1 \leq a \leq p - 1$.

Demostración. Si G_a es un conjugado de G_b por algún automorfismo $h \in \mathrm{Aut}\, A$ entonces $h \in N(\pi_2(G))$ y luego $h = \alpha_{l,i}\beta_{0,j}$. Entonces

$$\begin{aligned} h\tau\beta_{0,r}h^{-1} &= \tau^i\beta_{0,r} \in G_b \\ h\sigma^a\alpha_{1,1}h^{-1} &= \tau^{la}\sigma^a\alpha_{1,1}^i \in G_b. \end{aligned}$$

Luego $i = 1$ y $l = 0$ y tenemos que $a = b$.

Sea G un subgrupo regular con $|\pi_2(G)| = p^2$. En consecuencia, salvo conjugación, $\pi_2(G) = \langle \alpha_{1,1}, \beta_{0,r} \rangle$ y el núcleo de $\pi_2|_G$ es el subgrupo generado por ϵ. Luego, podemos suponer que

$$G = \langle \epsilon,\ \sigma^a \tau^b \alpha_{1,1},\ \sigma^c \tau^d \beta_{0,r} \rangle.$$

Por la condición (R), el segundo generador debe conmutar con el tercer generador módulo el núcleo, por lo cual tenemos que $c = 0$ y entonces $d \neq 0$ por regularidad. Si $a = 0$ entonces, por el lema 4.1.4(1), tenemos que $\pi_1(G) \subseteq \langle \tau, \epsilon \rangle$, una contradicción. En consecuencia $a \neq 0$ y G es un conjugado de G_a por el automorfismo $\alpha_{0,d^{-1}} \alpha_{1,1}^{-\frac{b}{a}}$. □

Lema 5.3.12. *Sea $p > 2$. Un conjunto de representantes de clases de conjugación de subgrupos regulares G de* $\mathrm{Hol}(A)$ *con $|\pi_2(G)| = p^2q$ es*

$$G_a = \langle \sigma \alpha_{1,1},\ \tau^a \beta_{0,r},\ \epsilon^{\frac{1}{r-1}} \beta_{1,1} \rangle \cong A$$

para $1 \leq a \leq p-1$.

Demostración. Si G_a y G_b son conjugados entre sí por h entonces h normaliza a $\langle \sigma \alpha_{1,1} \rangle$, el centro de G_a y G_b, y entonces $h = \beta_{0,j}$ para cierto j. Entonces $h \tau^a \beta_{0,r} h^{-1} = \tau^a \beta_{0,r} \in G_b$. En consecuencia $a = b$.

Sea G un subgrupo regular de $\mathrm{Hol}(A)$ con $|\pi_2(G)| = p^2q$. El único subgrupo de orden p^2q salvo conjugación es $\langle \alpha_{1,1}, \beta_{0,g}, \beta_{1,1} \rangle \cong A$. Luego, una presentación estándar de G es la siguiente:

$$G = \langle \epsilon^a u \alpha_{1,1},\ \epsilon^b v \beta_{0,r},\ \epsilon^c w \beta_{1,1} \rangle$$

para ciertos $u, v, w \in \langle \tau, \sigma \rangle$. Sea $u = \sigma^x \tau^y$. Como $\alpha_{1,1}$ es un elemento central en $\pi_2(G)$, por la condición (R), tenemos que $\epsilon^a u \alpha_{1,1} \in Z(G)$ y luego $v, w \in \langle \tau \rangle$ y

$$a = b\frac{r^x - 1}{r - 1} \quad \text{y} \quad c(r^x - 1) = \frac{r^x - 1}{r - 1}.$$

Ahora, levantando la relación $\beta_{0,r} \beta_{1,1} = \beta_{1,1}^r \beta_{0,r}$ tenemos que $w = 1$. Si $x = 0$, por el lema 4.1.4(1) tenemos $\pi_1(G) \subseteq \langle \epsilon, \tau \rangle$, una contradicción. Luego, supongamos que $x \neq 0$ y entonces $c = \frac{1}{r-1}$. Luego,

$$G = \langle \epsilon^{b\frac{r^x - 1}{r-1}} \sigma^x \tau^y \alpha_{1,1},\ \epsilon^b \tau^t \beta_{0,r},\ \epsilon^{\frac{1}{r-1}} \beta_{1,1} \rangle$$

para cierto $0 \leq t \leq p-1$. En consecuencia, usando (5.37) tenemos que G es un conjugado de G_{xt} por $h = \alpha_{n,x} \beta_{-b,1}$ donde $n = \frac{x-1}{2} - y$. □

La siguiente observación es análoga a la observación 5.1.15.

Observación 5.3.13. Las brazas torcidas de tipo A que se descomponen como producto directo son las siguientes:

(i) la braza torcida de la proposición 5.3.7.

(ii) La braza torcida asociada al grupo G_c para $1 \leq c \leq p-1$ como la definimos en el lema 5.3.8 es un producto directo de la braza torcida trivial de orden p y una braza torcida de orden pq con $|\ker \lambda| = q$, ver teorema 3.3.9.

(iii) La braza torcida asociada a G_a para $1 \leq a \leq p-1$ como la definimos en el lema 5.3.9 es el producto directo de la braza torcida trivial de orden p y una braza torcida de orden pq con $|\ker \lambda| = 1$, ver teorema 3.3.12.

Gracias a la enumeración de brazas torcidas de orden pq que conseguimos en los teoremas 3.3.6, 3.3.9 y 3.3.12, podemos decir que la observación anterior junto con la observación 5.1.15 nos dan una lista completa de las brazas torcidas de tipo no abeliano de orden p^2q que se pueden descomponer como un producto directo.

Resumimos el contenido de esta sección en las siguientes tablas.

$\lvert\ker\lambda\rvert$	$\mathbb{Z}_p^2 \times \mathbb{Z}_q$	$\mathbb{Z}_p \times (\mathbb{Z}_q \rtimes_g \mathbb{Z}_p)$
1	-	$p-1$
p	1	$2p-1$
q	-	$p-1$
pq	2	$2(p-1)$
p^2	1	-
p^2q	-	1

$\lvert\ker\lambda\rvert$	$\mathbb{Z}_{4q}$	$\mathbb{Z}_2^2 \times \mathbb{Z}_q$	$\mathbb{Z}_2 \times (\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_2)$	$\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_4$
2	1	-	2	1
$2q$	1	1	1	1
4	-	1	-	-
$4q$	-	-	1	-

Tabla 5.15: Enumeración de brazas torcidas de tipo A con la condición $q = 1 \pmod{p}$, $q \neq 1 \pmod{p^2}$: arriba asumimos que $p > 2$ y abajo, que $p = 2$.

5.4. Brazas torcidas de orden p^2q con $q = 1 \pmod{p^2}$

En esta sección podemos suponer que $q = 1 \pmod{p^2}$ y denotaremos por h a un elemento fijo de orden p^2 en $\mathbb{Z}_q^\times$. En consecuencia, tenemos los siguientes grupos no abelianos de orden p^2q:

(i) $\mathbb{Z}_q \rtimes_{h^p} \mathbb{Z}_{p^2} = \langle \sigma, \tau \,|\, \tau^q = \sigma^{p^2} = 1,\ \sigma\tau\sigma^{-1} = \tau^{h^p} \rangle$;

(ii) $\mathbb{Z}_p \times (\mathbb{Z}_q \rtimes_{h^p} \mathbb{Z}_p) = \langle \sigma, \tau, \epsilon \,|\, \sigma^p = \tau^p = \epsilon^q = 1,\ [\epsilon, \tau] = [\tau, \sigma] = 1,\ \sigma\epsilon\sigma^{-1} = \epsilon^{h^p} \rangle$;

(iii) $\mathbb{Z}_q \rtimes_h \mathbb{Z}_{p^2} = \langle \sigma, \tau \,|\, \tau^q = \sigma^{p^2} = 1,\ \sigma\tau\sigma^{-1} = \tau^h \rangle$.

En las tablas 5.16 y 5.17 resumimos la enumeración de brazas torcidas de acuerdo con la clase de isomorfismo de sus estructuras aditivas y multiplicativas.

$+\backslash\circ$	$\mathbb{Z}_{p^2q}$	$\mathbb{Z}_q \rtimes_{h^p} \mathbb{Z}_{p^2}$	$\mathbb{Z}_q \rtimes_h \mathbb{Z}_{p^2}$	$\mathbb{Z}_p^2 \times \mathbb{Z}_q$	$\mathbb{Z}_p \times (\mathbb{Z}_q \rtimes_{h^p} \mathbb{Z}_p)$
$\mathbb{Z}_q \rtimes_{h^p} \mathbb{Z}_{p^2}$	$2p$	$2p(p-1)$	$2p(p-1)$	-	-
$\mathbb{Z}_q \rtimes_h \mathbb{Z}_{p^2}$	2	$2(p-1)$	$2p(p-1)$	-	-
$\mathbb{Z}_p \times (\mathbb{Z}_q \rtimes_{h^p} \mathbb{Z}_p)$	-	-	-	4	$6p-4$

Tabla 5.16: Enumeración de brazas torcidas de orden p^2q con $q = 1 \pmod{p^2}$ para $p > 2$.

$+\backslash\circ$	$\mathbb{Z}_{4q}$	$\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_4$	$\mathbb{Z}_q \rtimes_h \mathbb{Z}_4$	$\mathbb{Z}_2^2 \times \mathbb{Z}_q$	$\mathbb{Z}_2 \times (\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_2)$
$\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_4$	2	2	2	2	4
$\mathbb{Z}_q \rtimes_h \mathbb{Z}_4$	2	2	4	-	-
$\mathbb{Z}_2 \times (\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_2)$	2	2	2	2	4

Tabla 5.17: Enumeración de brazas torcidas de orden $4q$ con $q = 1 \pmod{4}$.

Al igual que en la sección anterior, no seguiremos repitiendo la estrategia para verificar la regularidad de los subgrupos por ser demasiado repetitiva y rutinaria.

5.4.1. Brazas torcidas de tipo $\mathbb{Z}_q \rtimes_{h^p} \mathbb{Z}_{p^2}$

En esta sección denotaremos por A al grupo $\mathbb{Z}_q \rtimes_{h^p} \mathbb{Z}_{p^2}$. El grupo de automorfismos de A se puede describir como en la subsección 5.3.1 y utilizaremos la misma notación. En particular, los subgrupos de orden p, q y pq de $\operatorname{Aut} A$ coinciden con los subgrupos de la tabla 5.12. En consecuencia, si G es un subgrupo regular con $|\pi_2(G)| \in \{q, p, pq\}$ podemos aplicar los lemas 5.3.1, 5.3.2 y 5.3.3, respectivamente.

Salvo conjugación, los elementos de orden un divisor de p^2 están contenidos en el subgrupo de $\operatorname{Aut} A$ dado por $\langle \varphi_{1,0}^1,\ \varphi_{h,0}^0 \rangle \cong \mathbb{Z}_p \times \mathbb{Z}_p^2$. Entonces, de acuerdo con [66, Theorem 3.3], tenemos $p+1$ subgrupos de orden p^2, digamos

$$\langle \varphi_{h,0}^k \rangle \cong \mathbb{Z}_{p^2} \quad \text{y} \quad \langle \varphi_{1,0}^1,\ \varphi_{h^p,0}^0 \rangle \cong \mathbb{Z}_p \times \mathbb{Z}_p \tag{5.38}$$

para $0 \leq k \leq p-1$.

Por otro lado, como $\langle \varphi_{1,1}^0 \rangle$ es el único q-subgrupo de Sylow de $\operatorname{Aut} A$, tenemos que los subgrupos de orden p^2q de $\operatorname{Aut} A$ son los siguientes $p+1$ subgrupos salvo conjugación:

$$\langle \varphi_{h,0}^k,\ \varphi_{1,1}^0 \rangle \quad \text{y} \quad \langle \varphi_{1,0}^1,\ \varphi_{h^p,0}^0,\ \varphi_{1,1}^0 \rangle \tag{5.39}$$

para $0 \leq k \leq p-1$.

Los siguientes lemas enumeran los subgrupos regulares de $\operatorname{Hol}(A)$ salvo conjugación con $|\pi_2(G)| \in \{p^2, p^2q\}$. Para esto, separamos los casos $p = 2$ y $p > 2$.

Lema 5.4.1. *Sea $p > 2$. Un conjunto de representantes de clases de conjugación de subgrupos regulares G de* $\mathrm{Hol}(A)$ *con $|\pi_2(G)| = p^2$ es*

$$G_{b,k} = \langle \tau,\ \sigma^b \varphi_{h,0}^k \rangle \cong \mathbb{Z}_q \rtimes_h \mathbb{Z}_{p^2}$$

para $0 \leq k \leq p-1$ y $1 \leq b \leq p-1$.

Demostración. Análogamente al lema 5.3.2 podemos mostrar que los grupos no son conjugados entre sí. Sea G un subgrupo regular de $\mathrm{Hol}(A)$ con $|\pi_2(G)| = p^2$. El único subgrupo de orden q de A es $\langle \tau \rangle$. De acuerdo con (5.38) tenemos que considerar dos casos.

(i) Si $\pi_2(G) = \langle \varphi_{h,0}^k \rangle$ entonces una presentación estándar es la siguiente

$$G = \langle \tau, \tau^a \sigma^b \varphi_{h,0}^k \rangle = \langle \tau, \sigma^b \varphi_{h,0}^k \rangle$$

donde $b \neq 0 \pmod p$. Salvo conjugación por el normalizador de $\langle \varphi_{h,0}^k \rangle$ en $\mathrm{Aut}\, A$, podemos suponer que $1 \leq b \leq p-1$, luego $G = G_{b,k}$.

(ii) Si $\pi_2(G) = \langle \varphi_{1,0}^1,\ \varphi_{h^p,0}^0 \rangle$, entonces podemos argumentar como en la proposición 5.3.4 y probar que no existen subgrupos regulares bajo estas condiciones. □

Lema 5.4.2. *Sea $p > 2$. Un cojunto de representantes de clases de conjugación de subgrupos regulares G de* $\mathrm{Hol}(A)$ *con $|\pi_2(G)| = p^2q$ es*

$$G_{b,k} = \langle \sigma^b \varphi_{h,0}^k,\ \tau^{\frac{1}{h^p-1}} \varphi_{1,1}^0 \rangle \cong \mathbb{Z}_q \rtimes_h \mathbb{Z}_{p^2}$$

para $1 \leq b \leq p-1$ y $0 \leq k \leq p-1$.

Demostración. Los grupos no son conjugados entre sí por el mismo argumento del lema 5.3.2. Sea G un subgrupo regular de $\mathrm{Hol}(A)$ con $|\pi_2(G)| = p^2q$. De acuerdo con (5.39) debemos considerar dos casos. En el primero, G tiene la presentación estándar:

$$G = \langle \tau^a \sigma^b \varphi_{h,0}^k,\ \tau^c \sigma^d \varphi_{1,1}^0 \rangle.$$

Por la condición (R) $(\tau^a \sigma^b \varphi_{h,0}^k)^q = 1$ tenemos que $d = 0$ y entonces $b \neq 0 \pmod p$ (caso contrario, por el lema 4.1.4(1) se seguiría que $\pi_1(G) \subseteq \langle \sigma^p, \tau \rangle$). Más aún, podemos asumir también que $1 \leq b \leq p-1$, salvo conjugación por una potencia de $\varphi_{1,0}^1$. Por la condición (R), levantando la relación $\varphi_{h,0}^k \varphi_{1,1}^0 = (\varphi_{1,1}^0)^h \varphi_{h,0}^k$ tenemos que $c = \frac{1}{h^p-1}$.

Ahora, si $a = 0$, tenemos uno de los representantes del enunciado. Si no, conjugamos por $\varphi_{n,1}^0$ donde $n = -\frac{h^{pb+1}-1}{a(h^p-1)}$.

En el segundo caso no tenemos subgrupos regulares por el mismo argumento de la proposición 5.3.4. □

Ahora, vamos a tratar el caso $p = 2$. Recordemos que como h es un elemento de orden 4 en $\mathbb{Z}_q^\times$, podemos suponer que $h^2 = -1$.

Lema 5.4.3. *Sea $p = 2$. Un conjunto de representantes de clases de conjugación de subgrupos regulares G de* $\mathrm{Hol}(A)$ *con $|\pi_2(G)| = 4$ está dado por*

$$G_1 = \langle \tau,\ \sigma\varphi^1_{1,0},\ \sigma^2\varphi^0_{-1,0}\rangle \cong \mathbb{Z}_2 \times (\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_2), \qquad G_2 = \langle \tau,\ \sigma\varphi^0_{h,0}\rangle \cong \mathbb{Z}_q \rtimes_h \mathbb{Z}_4.$$

Demostración. Los grupos G_1 y G_2 no son conjugados entre sí pues sus imágenes por π_2 no lo son. Sea G un subgrupo regular de $\mathrm{Hol}(A)$. Si $\pi_2(G) = \langle \varphi^1_{1,0}, \varphi^0_{-1,0}\rangle$ podemos argumentar igual que en el lema 5.3.5 para conseguir G_1. Si $\pi_2(G) = \langle \varphi^k_{h,0}\rangle$ para $k = 0, 1$, argumentando como en el lema 5.4.1, tenemos

$$G = \langle \tau,\ \sigma\varphi^k_{h,0}\rangle.$$

Si $k = 1$ entonces $(\sigma\varphi^1_{h,0})^2 = (\varphi^1_{h,0})^2 = \varphi^0_{-1,1} \in G$ y luego G no es regular. En consecuencia, $k = 0$ y resulta $G = G_2$. □

Lema 5.4.4. *Sea $p = 2$. Existen dos subgrupos regulares de* $\mathrm{Hol}(A)$ *con $|\pi_2(G)| = 4q$ salvo conjugación. Un conjunto de representantes está dado por*

$$G_1 = \langle \sigma\varphi^1_{1,0},\ \sigma^2\varphi^0_{-1,0},\ \tau^{-\frac{1}{2}}\varphi^0_{1,1}\rangle \cong \mathbb{Z}_2 \times (\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_2)$$
$$y\ G_2 = \langle \sigma\varphi^0_{h,0},\ \tau^{-\frac{1}{2}}\varphi^0_{1,1}\rangle \cong \mathbb{Z}_q \rtimes_h \mathbb{Z}_4.$$

Demostración. Los grupos G_1 y G_2 no son conjugados pues sus imágenes por π_2 no lo son. Sea G un subgrupo regular de $\mathrm{Hol}(A)$. Si $\pi_2(G) = \langle \varphi^1_{1,0}, \varphi^0_{-1,0}, \varphi^0_{1,1}\rangle$, argumentando como en el lema 5.3.6 conseguimos G_1. Si $\pi_2(G) = \langle \varphi^k_{h,0},\ \varphi^0_{1,1}\rangle$, por el mismo argumento del lema 5.4.2, tenemos que G tiene la siguiente presentación estándar:

$$G = \langle \sigma\varphi^k_{h,0},\ \tau^{-\frac{1}{2}}\varphi^0_{1,1}\rangle.$$

Si $k = 1$ entonces $(\sigma\varphi^1_{h,0})^2 = (\varphi^1_{h,0})^2 = \varphi^0_{-1,0} \in G$ y luego G no es regular. Entonces $k = 0$ y conseguimos G_2. □

Los resultados de esta sección se resumen en las siguientes tablas:

$\lvert\ker\lambda\rvert$	$\mathbb{Z}_{p^2q}$	$\mathbb{Z}_q \rtimes_{h^p} \mathbb{Z}_{p^2}$	$\mathbb{Z}_q \rtimes_h \mathbb{Z}_{p^2}$
1	-	-	$p(p-1)$
p	$p-1$	$p(p-1)$	-
q	-	-	$p(p-1)$
p^2	1	-	-
pq	p	p^2-p-1	-
p^2q	-	1	-

$\lvert\ker\lambda\rvert$	$\mathbb{Z}_{4q}$	$\mathbb{Z}_2^2 \times \mathbb{Z}_q$	$\mathbb{Z}_2 \times (\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_2)$	$\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_4$	$\mathbb{Z}_q \rtimes_h \mathbb{Z}_4$
1	-	-	1	-	1
2	-	1	1	1	-
q	-	-	1	-	1
4	1	-	-	-	-
$2q$	1	1	1	-	-
$4q$	-	-	-	1	-

Tabla 5.18: Enumeración de brazas torcidas de tipo $\mathbb{Z}_q \rtimes_{h^p} \mathbb{Z}_{p^2}$ con la condición $q = 1 \pmod{p^2}$: arriba con $p > 2$ y abajo con $p = 2$.

5.4.2. Brazas torcidas de tipo $\mathbb{Z}_p \times (\mathbb{Z}_q \rtimes_{h^p} \mathbb{Z}_p)$

En esta sección denotamos por A al grupo $\mathbb{Z}_p \times (\mathbb{Z}_q \rtimes_{h^p} \mathbb{Z}_p)$. Los subgrupos regulares de $\mathrm{Hol}(A)$ con imágenes de órdenes q, p, pq por π_2 son los mismos de la proposición 5.3.7, el lema 5.3.8 y el lema 5.3.9, respetivamente, puesto que los subgrupos del grupo de automorfismos de A de orden p, q y pq coinciden con los del caso $q = 1 \pmod p$ y $q \neq 1 \pmod{p^2}$. Respetando la notación de la subsección 5.3.2, los subgrupos de orden p^2 de $\mathrm{Aut}\, A$ son

$$\langle \alpha_{1,1},\ \beta_{0,h^p} \rangle, \quad \langle \alpha_{1,1}^k \beta_{0,h} \rangle \tag{5.40}$$

para $0 \leq k \leq p-1$, salvo conjugación. Como hicimos antes, consideraremos los casos $p = 2$ y $p > 2$ en forma separada. Primero, comenzamos con el caso $p > 2$.

Lema 5.4.5. *Sea $p > 2$. Un conjunto de representantes de clases de conjugación de subgrupos regulares de* $\mathrm{Hol}(A)$ *con $|\pi_2(G)| = p^2$ es*

$$G_a = \langle \epsilon,\ \sigma^a \alpha_{1,1},\ \tau \beta_{0,h^p} \rangle \cong A$$

con $1 \leq a \leq p-1$.

Demostración. Si $\pi_2(G) = \langle \alpha_{1,1}, \beta_{0,h^p} \rangle$ podemos argumentar como en el lema 5.3.11 para obtener a G_a. Mostraremos que si $\pi_2(G) = \langle \alpha_{1,1}^k \beta_{0,h} \rangle$ para $0 \leq k \leq p-1$ entonces G no es regular. Podemos suponer que

$$G = \langle \epsilon,\ \sigma^a \tau^b \alpha_{1,1}^k \beta_{0,h} \rangle.$$

Si $k = 0$ entonces $(\sigma^a \tau^b \beta_{0,h})^p = \beta_{0,h}^p \in G$. Caso contrario, como $p > 2$, tenemos que

$$(\sigma^a \tau^b \alpha_{1,1}^k \beta_{0,h})^p = \tau^{bp + k\frac{p(p-1)a}{2}} \sigma^{ap} \alpha_{1,1}^{pk} \beta_{0,h}^p = \beta_{0,h}^p \in G.$$

En ambos casos, G no es regular por el lema 4.1.3. □

Ahora veamos el caso $p = 2$. En este caso, tenemos que $h^2 = -1$.

Lema 5.4.6. *Sea $p = 2$. Existe una única clase de conjugación de subgrupos regulares de* $\mathrm{Hol}(A)$ *con $|\pi_2(G)| = 4$. Un representante es*

$$H = \langle \epsilon,\ \sigma \alpha_{1,1} \beta_{0,h} \rangle \cong \mathbb{Z}_q \rtimes_h \mathbb{Z}_4.$$

Demostración. Si $\pi_2(G)$ está generado por $\alpha_{1,1}$ y $\beta_{0,-1}$ entonces G no es regular por los mismos cálculos de la proposición 5.3.10. Supongamos que $\pi_2(G) = \langle \alpha_{1,1}^k \beta_{0,h} \rangle$ para $k = 0, 1$, entonces G tiene la siguiente presentación estándar

$$G = \langle \epsilon,\ \sigma^a \tau^b \alpha_{1,1}^k \beta_{0,h} \rangle$$

para ciertos $0 \leq a, b \leq 1$. Si $k = 0$ entonces $(\sigma^a \tau^b \beta_{0,h})^2 = \beta_{0,h}^2 = \beta_{0,-1} \in G$ y luego G no es regular. Entonces $k = 1$ y $a = 1$, caso contrario tendríamos $\pi_1(G) \subseteq \langle \tau, \epsilon \rangle$. Por último, podemos suponer que $b = 0$ salvo conjugación por $\alpha_{1,1}$. □

Los subgrupos de orden p^2q en $\operatorname{Aut} A$ son

$$\langle \alpha_{1,1},\ \beta_{0,h^p},\ \beta_{1,1}\rangle, \quad \langle \beta_{1,1},\ \alpha_{1,1}^k\beta_{0,h}\rangle$$

para $0 \leq k \leq p-1$, salvo conjugación. Consideramos además los casos $p > 2$ y $p = 2$ por separado. Comencemos con el caso $p > 2$.

Lema 5.4.7. *Sea $p > 2$. Un conjunto de representantes de clases de conjugación de subgrupos regulares de* $\operatorname{Hol}(A)$ *con $|\pi_2(G)| = p^2q$ es*

$$G_a = \langle \sigma\alpha_{1,1},\ \tau^a\beta_{0,h^p},\ \epsilon^{\frac{1}{h^p-1}}\beta_{1,1}\rangle \cong A$$

para $1 \leq a \leq p-1$.

Demostración. Si el p-subgrupo de Sylow de la imagen $\pi_2(G)$ no es cíclico podemos concluir como en el lema 5.3.12. Veamos que si $\pi_2(G) = \langle \beta_{1,1},\ \alpha_{1,1}^k\beta_{0,h}\rangle$ entonces G no es regular. En efecto, si

$$G = \langle \epsilon^a u\beta_{1,1},\ \epsilon^b v\alpha_{1,1}^k\beta_{0,h}\rangle$$

para ciertos $u, v \in \langle \sigma, \tau\rangle$ entonces, como $(\epsilon^a u\beta_{1,1})^q = 1$ por la condición (R), tenemos que $u = 1$, es decir $G = \langle \epsilon^a\beta_{1,1},\ \epsilon^b v\alpha_{1,1}^k\beta_{0,h}\rangle$ donde $v = \sigma^c\tau^d$. Más aún, podemos suponer que $a \neq 0$ por regularidad. Como $p > 2$, tenemos que

$$(\epsilon^b\sigma^c\tau^d\alpha_{1,1}^k\beta_{0,h})^p = \epsilon^s\tau^{dp+ck\frac{p(p-1)}{2}}\sigma^{cp}\alpha_{1,1}^{kp}\beta_{0,h}^p = \epsilon^s\beta_{0,h}^p \in G$$

para algún s. Luego,

$$(\epsilon^a\beta_{1,1})^{-\frac{s}{a}}(\epsilon^s\beta_{0,h}^p) = \beta_{1,1}^{-\frac{s}{a}}\beta_{0,h}^p \in G$$

y entonces G no es regular. □

Lema 5.4.8. *Sea $p = 2$. Existe una única clase de conjugación de subgrupos regulares de* $\operatorname{Hol}(A)$ *con $|\pi_2(G)| = 4q$. Un representante es*

$$H = \langle \sigma\alpha_{1,1}\beta_{0,h},\ \epsilon^{-\frac{1}{2}}\beta_{1,1}\rangle \cong \mathbb{Z}_q \rtimes_h \mathbb{Z}_4.$$

Demostración. Si $\pi_2(G) = \langle \alpha_{1,1},\ \beta_{0,-1},\ \beta_{1,1}\rangle$ entonces G no es regular por los mismos cálculos de la proposición 5.3.10. Supongamos que $\pi_2(G) = \langle \alpha_{1,1}^k\beta_{0,h},\ \beta_{1,1}\rangle$ para $k = 0, 1$, luego G tiene la siguiente presentación estándar

$$\langle \tau^a\epsilon^b\sigma^c\alpha_{1,1}^k\beta_{0,h},\ \tau^d\epsilon^e\sigma^f\beta_{1,1}\rangle$$

para ciertos $0 \leq a, c, d, f \leq 1$ y $0 \leq b, e \leq q-1$. Por la condición (R), como $(\tau^d\epsilon^e\sigma^f\beta_{1,1})^q = 1$ tenemos que $f = d = 0$. Por regularidad, $e \neq 0 \pmod{q}$. Si $c = 0$ entonces $\pi_1(G) \subseteq \langle \tau, \epsilon\rangle$. Luego, $c = 1$. Por la condición (R) y el hecho de que $\beta_{0,h}\beta_{1,1} = \beta_{1,1}^h\beta_{0,h}$, tenemos que $e = -\frac{1}{2}$. Salvo conjugación por $\alpha_{1,1}$ podemos suponer que $a = 0$.

Si $k = 0$ entonces $(\epsilon^{-\frac{1}{2}}\beta_{1,1})^{-2b(h-1)}(\epsilon^b\sigma\beta_{0,h})^2 = \beta_{1,1}^{-2b(h-1)}\beta_{0,h}^2 \in G$ y en consecuencia G no es regular. Luego, $k = 1$ y G es un conjugado de H por $\beta_{1,1}^n$ donde $n = -\frac{2b}{h+1}$. □

De acuerdo con los lemas 5.4.5 y 5.4.7, la tabla 5.15 recolecta la enumeración de brazas torcidas de tipo $\mathbb{Z}_p \times (\mathbb{Z}_q \rtimes_{h^p} \mathbb{Z}_p)$ con $q = 1 \pmod{p^2}$ y $p > 2$. En la tabla 5.19 se reúne la enumeración para el caso $p = 2$.

$\ker \lambda$	$\mathbb{Z}_{4q}$	$\mathbb{Z}_2^2 \times \mathbb{Z}_q$	$\mathbb{Z}_2 \times (\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_2)$	$\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_4$	$\mathbb{Z}_q \rtimes_h \mathbb{Z}_4$
1	-	-	-	-	1
2	1	-	2	1	-
4	-	1	-	-	-
q	-	-	-	-	1
$2q$	1	1	1	1	-
$4q$	-	-	1	-	-

Tabla 5.19: Enumeración de brazas torcidas de tipo $\mathbb{Z}_2 \times (\mathbb{Z}_q \rtimes_{-1} \mathbb{Z}_2)$ con $q = 1 \pmod 4$.

5.4.3. Brazas torcidas de tipo $\mathbb{Z}_q \rtimes_h \mathbb{Z}_{p^2}$

En esta sección, denotaremos por A al grupo $\mathbb{Z}_q \rtimes_h \mathbb{Z}_{p^2}$. Una presentación de este grupo es

$$G = \langle \sigma, \tau \mid \sigma^{p^2} = \tau^q = 1,\ \sigma\tau\sigma^{-1} = \tau^h \rangle.$$

De acuerdo con [17, Theorem 3.4], la función

$$\phi : \mathbb{Z}_q \rtimes \mathbb{Z}_q^\times \longrightarrow \operatorname{Aut} A, \quad (i,j) \mapsto \varphi_{i,j} = \begin{cases} \tau \mapsto \tau^j \\ \sigma \mapsto \tau^i \sigma \end{cases}$$

es un isomorfismo de grupos.

Como $q = 1 \pmod{p^2}$ entonces p^2q divide a $|\operatorname{Aut} G| = q(q-1)$ y debemos discutir todos los posibles valores para $|\pi_2(G)|$.

Un conjunto de representantes de clases de conjugación de subgrupos de $\operatorname{Aut} A$ lo podemos ver en la tabla 5.20.

Orden	Grupo	Clase
p	$\langle \varphi_{0,h^p} \rangle$	$\mathbb{Z}_p$
q	$\langle \varphi_{1,1} \rangle$	$\mathbb{Z}_q$
pq	$\langle \varphi_{0,h^p},\ \varphi_{1,1} \rangle$	$\mathbb{Z}_q \rtimes_{h^p} \mathbb{Z}_p$
p^2	$\langle \varphi_{0,h} \rangle$	$\mathbb{Z}_{p^2}$
p^2q	$\langle \varphi_{1,1},\ \varphi_{0,h} \rangle$	A

Tabla 5.20: Clases de conjugación de subgrupos de $\operatorname{Aut} A$.

Lema 5.4.9. *La única braza torcida de tipo A con* $|\ker\lambda| = p^2$ *es* $(B, +, \circ)$ *donde*

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} x_1 + h^{x_2} y_1 \\ x_2 + y_2 \end{pmatrix}, \qquad \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \circ \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} h^{y_2} x_1 + h^{x_2} y_1 \\ x_2 + y_2 \end{pmatrix}$$

para todos $0 \leq x_1, y_1 \leq q-1$ *y* $0 \leq x_2, y_2 \leq p^2 - 1$. *En particular,* $(B, \circ) \cong \mathbb{Z}_{p^2q}$.

Demostración. Sea G un subgrupo regular de $\mathrm{Hol}(A)$ con $|\pi_2(G)| = q$. Entonces podemos suponer que $\pi_2(G) = \langle \varphi_{1,1} \rangle$ que es normal en $\operatorname{Aut} A$.

Como todos los p-subgrupos de Sylow de A son conjugados entre sí y tienen orden p^2, podemos suponer que G tiene la presentación estándar

$$G = \langle \sigma,\ \tau^a \sigma^b \varphi_{1,1} \rangle = \langle \sigma,\ \tau^a \varphi_{1,1} \rangle,$$

para cierto $a \neq 0$. La condición (K) se satisface si y sólo si $a = \frac{1}{h-1}$.

La fórmula para la braza torcida asociada a G se puede obtener como en el lema 5.3.1. □

El grupo $\mathfrak{G}_3 = \langle \tau, \varphi_{1,1} \rangle$ es normal en $\mathrm{Hol}(A)$ y $\mathrm{Hol}(A)/\mathfrak{G}_3 \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_q^\times$.

Lema 5.4.10. *Las brazas torcida de tipo A con* $|\ker\lambda| = pq$ *son* $(B_c, +, \circ)$ *donde* $(B_c, +) = \mathbb{Z}_q \rtimes_h \mathbb{Z}_{p^2}$ *y* $(B_c, \circ) = \mathbb{Z}_q \rtimes_{h^{\frac{p}{c}+1}} \mathbb{Z}_{p^2} \cong A$ *for* $1 \leq c \leq p-1$. *En particular,* B_c *es una bi-braza.*

Demostración. El subgrupo

$$G_c = \langle \tau,\ \sigma^p,\ \sigma^c \varphi_{0,h^p} \rangle \cong A$$

es regular. Si G_c y G_d son conjugados entre sí entonces sus imágenes en $\mathrm{Hol}(A)/\mathfrak{G}_3$ coinciden y luego $\langle \sigma^p, \sigma^c \varphi_{0,h^p} \rangle = \langle \sigma^p, \sigma^d \varphi_{0,h^p} \rangle$. En consecuencia, $c = d$.

El único subgrupo de A de orden pq es $\langle \tau, \sigma^p \rangle$. Luego, si G es un subgrupo regular de $\mathrm{Hol}(A)$, podemos suponer que $G = G_c$ para algún $1 \leq c \leq p-1$.

Usando el mismo argumento del lema 5.1.4 podemos describir la estructura de la braza torcida B_c asociada a G_c y de acuerdo con el corolario 3.1.2, la braza torcida asociada es una bi-braza. □

Lema 5.4.11. *Un conjunto de representantes de clases de conjugación de subgrupos regulares de* $\mathrm{Hol}(A)$ *tal que* $|\pi_2(G)| = pq$ *es*

$$G_c = \langle \sigma^p,\ \sigma^c \varphi_{0,h^p},\ \tau^{\frac{1}{h-1}} \varphi_{1,1} \rangle \cong A$$

para $1 \leq c \leq p-1$.

Demostración. Al igual que en el lema 5.4.10 podemos mostrar que los grupos G_c no son conjugados entre sí. Sea G un subgrupo regular de $\mathrm{Hol}(A)$ con $|\pi_2(G)| = pq$. De acuerdo con la tabla 5.20, podemos suponer que $\pi_2(G) = \langle \varphi_{0,h^p},\ \varphi_{1,1} \rangle$. Los subgrupos de orden p de A son $\langle \tau^a \sigma^p \rangle$ para algún a. Como $\varphi_{1,1}$ está en el normalizador de $\pi_2(G)$,

salvo conjugación por una potencia de $\varphi_{1,1}$ podemos suponer que $a = 0$. Luego, G tiene la siguiente presentación estándar

$$G = \langle \sigma^p,\ \tau^b\sigma^c\varphi_{0,h^p},\ \tau^d\sigma^e\varphi_{1,1}\rangle$$

para ciertos $0 \leq c, e \leq p-1$ y $0 \leq b, d \leq q-1$. Por la condición (R) y el hecho de que $\varphi_{0,h^p}\varphi_{1,1} = \varphi_{1,1}^{h^p}\varphi_{0,h^p}$ se sigue que $e(1-h^p) = 0 \pmod{p^2}$, luego $e = 0 \pmod{p}$, y $d(h^c-1) = \frac{h^c-1}{h-1}$. Si $c = 0$ entonces $\pi_1(G) \subseteq \langle \tau, \sigma^p\rangle$ por el lema 4.1.4(1), por lo cual tenemos que $c \neq 0$ y entonces $d = \frac{1}{h-1}$. Por $(\tau^b\sigma^c\varphi_{0,h^p})^p \in \langle \sigma^p\rangle$ conseguimos $b = 0$. En consecuencia, $G = G_c$. □

Lema 5.4.12. *Un conjunto de representantes de clases de conjugación de subgrupos regulares de* $\mathrm{Hol}(A)$ *con* $|\pi_2(G)| = p^2$ *es*

$$G_b = \langle \tau,\ \sigma^b\varphi_{0,h}\rangle \cong \begin{cases} \mathbb{Z}_{p^2q}, & \text{si } b = -1 \pmod{p^2}, \\ \mathbb{Z}_q \rtimes_{h^p} \mathbb{Z}_{p^2}, & \text{si } b = -1 \pmod{p} \text{ y } b \neq -1 \pmod{p^2}, \\ \mathbb{Z}_q \rtimes_h \mathbb{Z}_{p^2}, & \text{en otro caso,} \end{cases}$$

donde $1 \leq b \leq p^2-1$ *y* $b \neq 0 \pmod{p}$.

Demostración. Por el mismo argumento del lema 5.4.10, los grupos no son conjugados entre sí. Sea G un subgrupo regular de $\mathrm{Hol}(A)$ con $|\pi_2(G)| = p^2$. Como A tiene un único subgrupo de orden q, de acuerdo con la tabla 5.20, tenemos que todo subgrupo regular G tiene la presentación estándar

$$G_b = \langle \tau,\ \sigma^b\varphi_{0,h}\rangle$$

para $b \neq 0 \pmod{p}$ (en otro caso, tendríamos $\pi_1(G) \subseteq \langle \tau, \sigma^p\rangle$), es decir $G = G_b$. □

Lema 5.4.13. *Un conjunto de representantes de clases de conjugación de subgrupos regulares* G *de* $\mathrm{Hol}(A)$ *con* $|\pi_2(G)| = p^2q$ *es*

$$G_d = \langle \tau^{\frac{1}{h-1}}\varphi_{1,1},\ \sigma^d\varphi_{0,h}\rangle \cong A$$

para $1 \leq d \leq p^2-1$ *y* $d \neq 0 \pmod{p}$.

Demostración. Sea G un subgrupo regular con $|\pi_2(G)| = p^2q$. De acuerdo con la tabla 5.20, podemos suponer que una presentación estándar es

$$G = \langle \tau^a\sigma^b\varphi_{1,1},\ \tau^c\sigma^d\varphi_{0,h}\rangle.$$

Gracias a las condiciones (R), de $(\tau^a\sigma^b\varphi_{1,1})^q = 1$ obtenemos $b = 0$. Levantando la relación $\varphi_{0,h}\varphi_{1,1} = \varphi_{1,1}^h\varphi_{0,h}$, conseguimos la ecuación $a(h^d-1) = \frac{h^d-1}{h-1}$.

Si $d = 0 \pmod{p}$ entonces $\pi_1(G) \subseteq \langle \tau, \sigma^p\rangle$. Luego $d \neq 0 \pmod{p}$ y $a = \frac{1}{h-1}$. Entonces,

$$G = \langle \tau^{\frac{1}{h-1}}\varphi_{1,1},\ \tau^c\sigma^d\varphi_{0,h}\rangle$$

para $d \neq 0 \pmod{p}$. Si $d = -1$ entonces $c = 0$ puesto que $\tau^c\sigma^d\varphi_{0,h}$ tiene orden p^2. En otro caso, G es un conjugado de G_d por $\varphi_{-c\frac{h-1}{h^{d+1}-1},1}$. □

Resumimos el contenido de esta subsección en la siguiente tabla:

$\lvert\ker\lambda\rvert$	$\mathbb{Z}_{p^2q}$	$\mathbb{Z}_q \rtimes_{h^p} \mathbb{Z}_{p^2}$	$\mathbb{Z}_q \rtimes_h \mathbb{Z}_{p^2}$
1	-	-	$p(p-1)$
p	-	$p-1$	-
q	1	$p-1$	$p(p-2)$
p^2	1	-	-
pq	-	-	$p-1$
p^2q	-	-	1

Tabla 5.21: Enumeración de brazas torcidas de tipo $\mathbb{Z}_q \rtimes_h \mathbb{Z}_{p^2}$ para $q = 1 \pmod{p^2}$.

5.5. Una demostración de una conjetura de brazas torcidas de orden p^2q

En esta sección, daremos una demostración positiva para la conjetura 4.1 de [13]. Para ello, necesitaremos todas las tablas que conseguimos al enumerar las brazas torcidas de orden p^2q en los capítulos 4 y 5.

Dado un entero n, denotamos por $A(n)$ la cantidad de brazas torcidas de tipo abeliano de orden n no isomorfas entre sí. (es decir, las brazas clásicas) y por $B(n)$ a la cantidad de brazas torcidas de tipo no abeliano de orden n no isomorfas entre sí. Luego, la cantidad total de brazas torcidas no isomorfas entre sí de orden n es:

$$s(n) = A(n) + B(n). \tag{5.41}$$

Por [29], se conoce el valor de $A(4q)$ para un primo $q \geq 5$ y también el valor de $A(p^2q)$ para primos p, q con la condición $q > p + 1 > 3$. Volveremos a probar estos resultados como un caso particular.

Teorema 5.5.1. *[13, Conjecture 4.1] Sean p y q números primos. Si $q \geq 5$ entonces*

$$s(4q) = \begin{cases} 29, & si\ q = 3 \pmod 4 \\ 43, & si\ q = 1 \pmod 4 \end{cases}$$

y si $q > p + 1 > 3$, entonces

$$s(p^2q) = \begin{cases} 4, & si\ q \neq 1 \pmod p \\ 2p^2 + 7p + 8, & si\ q = 1 \pmod p\ y\ q \neq 1 \pmod{p^2} \\ 6p^2 + 6p + 8, & si\ q = 1 \pmod{p^2}. \end{cases}$$

Demostración. Para la primera parte, de acuerdo con la tabla 4.1 tenemos que

$$A(4q) = \begin{cases} 9, & \text{si } q = 3 \pmod 4 \\ 11, & \text{si } q = 1 \pmod 4 \end{cases}$$

y sumando todas las entradas de las tablas 5.11 y 5.17, conseguimos:

$$B(4q) = \begin{cases} 20, & \text{si } q = 3 \pmod 4 \\ 32, & \text{si } q = 1 \pmod 4. \end{cases}$$

Luego, por (5.41) conseguimos el valor deseado de $s(4q)$.

Para la segunda parte, de acuerdo con [14, p. 237], tenemos que las condiciones $q > p + 1 > 3$ y $q \neq 1 \pmod p$ sólo pueden cumplirse simultáneamente si p y q son aritméticamente independientes (es decir $p \neq \pm 1 \pmod q$ y $q \neq 1 \pmod p$). Luego, por la tabla 4.1 tenemos:

$$A(p^2q) = \begin{cases} 4, & \text{si } q \neq 1 \pmod p \\ p + 8, & \text{si } q = 1 \pmod p \text{ y } q \neq 1 \pmod{p^2} \\ 2p + 8, & \text{si } q = 1 \pmod{p^2}. \end{cases}$$

Para $B(n)$, el caso $q = 1 \pmod p$ y $q \neq 1 \pmod{p^2}$ proviene de la tabla 5.10 y la condición $q = 1 \pmod{p^2}$ proviene de la tabla 5.16. Por último, como todo grupo de orden p^2q con p y q aritméticamente independientes debe ser abeliano, sólo tenemos brazas torcidas de tipo abeliano. En resumen:

$$B(p^2q) = \begin{cases} 0, & \text{si } q \neq 1 \pmod p \\ 2p^2 + 6p, & \text{si } q = 1 \pmod p \text{ y } q \neq 1 \pmod{p^2} \\ 6p^2 + 4p, & \text{si } q = 1 \pmod{p^2} \end{cases}$$

y entonces se sigue la segunda parte de la conjetura. Notemos que los últimos números de la enumeración los conseguimos sumando todas las entradas de las tablas 5.10 y 5.16. □

En [41], los autores realizan una serie de conjeturas a partir de los resultados que obtuvieron mediante cálculos computacionales. Todas ellas fueron probadas por separado en [60] y [29]. Dado que se trata de brazas (de tipo abeliano) de orden p^2q, nuestro trabajo da una nueva demostración como aplicación del teorema anterior. Adaptando los enunciados a nuestra notación tenemos que:

- [41, Conjecture 6.2] trata sobre la cantidad de brazas de orden $4q$ que probamos en el teorema 5.5.1 como $A(4q)$;
- [41, Conjecture 6.3] trata sobre la cantidad de brazas de orden $9q$ que también vimos en el teorema 5.5.1. Tomando $p = 3$ conseguimos

$$A(9q) = \begin{cases} 4, & \text{si } q \neq 1 \pmod 3 \\ 11, & \text{si } q = 1 \pmod 3 \text{ y } q \neq 1 \pmod 9 \\ 14, & \text{si } q = 1 \pmod 9. \end{cases}$$

- [41, Conjecture 6.4] afirma que $A(p^2q) = 4$ si $p < q$ y $q \neq 1 \pmod p$, como se deduce de la demostración del teorema 5.5.1.

Índice alfabético

Notación

a'	inverso de a para la operación $\circ$, 4
$A^{(n)}$	sucesión de ideales, 12
A^n	sucesión de ideales a izquierda, 13
$\mathrm{Aut}(A)$	grupo de automorfismos del grupo A, 13
$\mathfrak{B}$	subconjunto de $\mathbb{Z}_q$, 49
$C_G(A)$	centralizador de un subgrupo A de G, 13
$Z(A,+)$	centro del grupo A, 8
$[x,y]_+$	conmutador de x e y, 12
$e'(G,A,m)$	cantidad de subgrupos regulares de $\mathrm{Hol}(A)$ isomorfos a G con imagen por π_2 de orden m, 36
$*$	operación estrella, 6
η	automorfismo -1 del grupo $\mathbb{Z}_2^2 \times \mathbb{Z}_q$, 66
ϕ	función ϕ de Euler, 38
$\mathrm{Fix}(A)$	ideal a izquierda $\mathrm{Fix}(A)$ de una braza, 8
f_j	función biyectiva del lema 4.5.2, 63
g	elemento de orden q en $\mathbb{Z}_p^\times$
$\mathcal{G}_F$	grupo isomorfo a $\mathbb{Z}_p^2 \rtimes_F \mathbb{Z}_q$, 56
$\mathcal{G}_k$	grupo isomorfo a $\mathbb{Z}_p^2 \rtimes_{\mathcal{D}_{1,k}} \mathbb{Z}_q$, 49
$G(X,r)$	grupo de estructura, 7
$\mathcal{G}(X,r)$	grupo de permutaciones, 7
$GL_2(p)$	grupo de automorfismos de $\mathbb{Z}_p^2$
h	elemento de orden p^2 en $\mathbb{Z}_{p^2}^\times$, 62

Bibliografía

[1] E. Acri and M. Bonatto. Skew braces of size pq. *Commun. Algebra*, 48(5):1872–1881, 2020.

[2] E. Acri and M. Bonatto. Skew braces of size p^2q. II: Non-abelian type. *J. Algebra Appl.*, 21(3):61, 2022. Id/No 2250062.

[3] E. Acri and M. Bonatto. Skew braces of size p^2q. I: Abelian type. *Algebra Colloq.*, 29(2):297–320, 2022.

[4] E. Acri, R. Lutowski, and L. Vendramin. Retractability of solutions to the Yang-Baxter equation and p-nilpotency of skew braces. *Int. J. Algebra Comput.*, 30(1):91–115, 2020.

[5] Ö. Akgün, M. Mereb, and L. Vendramin. Enumeration of set-theoretic solutions to the Yang-Baxter equation. *Math. Comput.*, 91(335):1469–1481, 2022.

[6] A. A. Alabdali and N. P. Byott. Skew braces of squarefree order. *J. Algebra Appl.*, 20(7):21, 2021. Id/No 2150128.

[7] D. Bachiller. Classification of braces of order p^3. *J. Pure Appl. Algebra*, 219(8):3568–3603, 2015.

[8] D. Bachiller. Counterexample to a conjecture about braces. *J. Algebra*, 453:160–176, 2016.

[9] D. Bachiller. Solutions of the Yang-Baxter equation associated to skew left braces, with applications to racks. *J. Knot Theory Ramifications*, 27(8):36, 2018. Id/No 1850055.

[10] D. Bachiller, F. Cedó, and E. Jespers. Solutions of the Yang-Baxter equation associated with a left brace. *J. Algebra*, 463:80–102, 2016.

[11] D. Bachiller, F. Cedó, E. Jespers, and J. Okniński. A family of irretractable square-free solutions of the Yang-Baxter equation. *Forum Math.*, 29(6):1291–1306, 2017.

[12] D. Bachiller, F. Cedó, and L. Vendramin. A characterization of finite multipermutation solutions of the Yang-Baxter equation. *Publ. Mat., Barc.*, 62(2):641–649, 2018.

[13] V. G. Bardakov, M. V. Neshchadim, and M. K. Yadav. Computing skew left braces of small orders. *Int. J. Algebra Comput.*, 30(4):839–851, 2020.

[14] S. R. Blackburn, P. M. Neumann, and G. Venkataraman. *Enumeration of finite groups*, volume 173 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2007.

[15] N. P. Byott. Uniqueness of Hopf Galois structure for separable field extensions. *Commun. Algebra*, 24(10):3217–3228, 1996.

[16] N. P. Byott. Hopf-Galois structures on Galois field extensions of degree pq. *J. Pure Appl. Algebra*, 188(1-3):45–57, 2004.

[17] E. Campedel, A. Caranti, and I. Del Corso. The automorphism groups of groups of order p^2q. *Int. J. Group Theory*, 10(3):149–157, 2021.

[18] F. Cedó, T. Gateva-Ivanova, and A. Smoktunowicz. On the Yang-Baxter equation and left nilpotent left braces. *J. Pure Appl. Algebra*, 221(4):751–756, 2017.

[19] F. Cedó, E. Jespers, and Á. del Río. Involutive Yang-Baxter groups. *Trans. Am. Math. Soc.*, 362(5):2541–2558, 2010.

[20] F. Cedó, E. Jespers, and J. Okniński. Retractability of set theoretic solutions of the Yang-Baxter equation. *Adv. Math.*, 224(6):2472–2484, 2010.

[21] F. Cedó, E. Jespers, and J. Okniński. An abundance of simple left braces with abelian multiplicative Sylow subgroups. *Rev. Mat. Iberoam.*, 36(5):1309–1332, 2020.

[22] F. Cedó, A. Smoktunowicz, and L. Vendramin. Skew left braces of nilpotent type. *Proc. Lond. Math. Soc. (3)*, 118(6):1367–1392, 2019.

[23] L. N. Childs. Bi-skew braces and Hopf–Galois structures. *New York J. Math.*, 25:574–588, 2019.

[24] F. Chouraqui. Garside groups and Yang-Baxter equation. *Commun. Algebra*, 38(12):4441–4460, 2010.

[25] F. Chouraqui. Left orders in Garside groups. *Int. J. Algebra Comput.*, 26(7):1349–1359, 2016.

[26] F. Chouraqui and E. Godelle. Finite quotients of groups of I-type. *Adv. Math.*, 258:46–68, 2014.

[27] T. Crespo and M. Salguero. Computation of Hopf Galois structures on separable extensions and classification of those for degree twice an odd prime power. *J. Algebra Appl.*, 20(4):13, 2021. Id/No 2150049.

[28] P. Dehornoy. Set-theoretic solutions of the Yang-Baxter equation, RC-calculus, and Garside germs. *Adv. Math.*, 282:93–127, 2015.

[29] C. Dietzel. Braces of order p^2q. *J. Algebra Appl.*, 20(8):24, 2021. Id/No 2150140.

[30] V. G. Drinfel'd. On some unsolved problems in quantum group theory. In *Quantum groups. Proceedings of workshops, held in the Euler International Mathematical Institute, Leningrad, USSR, Fall 1990*, pages 1–8. Berlin etc.: Springer-Verlag, 1992.

[31] P. Etingof, T. Schedler, and A. Soloviev. Set-theoretical solutions to the quantum Yang-Baxter equation. *Duke Math. J.*, 100(2):169–209, 1999.

[32] D. R. Farkas. Crystallographic groups and their mathematics. *Rocky Mt. J. Math.*, 11:511–551, 1981.

[33] A. Gąsior, R. Lutowski, and A. Szczepański. A short note about diffuse Bieberbach groups. *J. Algebra*, 494:237–245, 2018.

[34] T. Gateva-Ivanova. Quadratic algebras, Yang-Baxter equation, and Artin-Schelter regularity. *Adv. Math.*, 230(4-6):2152–2175, 2012.

[35] T. Gateva-Ivanova. Set-theoretic solutions of the Yang-Baxter equation, braces and symmetric groups. *Adv. Math.*, 338:649–701, 2018.

[36] T. Gateva-Ivanova. A combinatorial approach to noninvolutive set-theoretic solutions of the Yang-Baxter equation. *Publ. Mat., Barc.*, 65(2):747–808, 2021.

[37] T. Gateva-Ivanova and P. Cameron. Multipermutation solutions of the Yang-Baxter equation. *Commun. Math. Phys.*, 309(3):583–621, 2012.

[38] T. Gateva-Ivanova and S. Majid. Quantum spaces associated to multipermutation solutions of level two. *Algebr. Represent. Theory*, 14(2):341–376, 2011.

[39] T. Gateva-Ivanova and M. Van den Bergh. Semigroups of I-type. *J. Algebra*, 206(1):97–112, 1998.

[40] M. Ghorbani and F. N. Larki. Automorphism group of groups of order pqr. *Algebr. Struct. Appl.*, 1(1):49–56, 2014.

[41] L. Guarnieri and L. Vendramin. Skew braces and the Yang-Baxter equation. *Math. Comput.*, 86(307):2519–2534, 2017.

[42] I. M. Isaacs. *Finite group theory*, volume 92 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2008.

[43] E. Jespers and J. Okniński. Monoids and groups of I-type. *Algebr. Represent. Theory*, 8(5):709–729, 2005.

[44] E. Jespers and J. Okniński. *Noetherian semigroup algebras*, volume 7 of *Algebras and Applications*. Springer, Dordrecht, 2007.

[45] S. Kionke and J. Raimbault. On geometric aspects of diffuse groups. With an appendix by Nathan Dunfield. *Doc. Math.*, 21:873–915, 2016.

[46] T. Kohl. Groups of order $4p$, twisted wreath products and Hopf-Galois theory. *J. Algebra*, 314(1):42–74, 2007.

[47] A. Konovalov, A. Smoktunowicz, and L. Vendramin. On skew braces and their ideals. *Exp. Math.*, 30(1):95–104, 2021.

[48] V. Lebed and L. Vendramin. On structure groups of set-theoretic solutions to the Yang-Baxter equation. *Proc. Edinb. Math. Soc., II. Ser.*, 62(3):683–717, 2019.

[49] J.-H. Lu, M. Yan, and Y.-C. Zhu. On the set-theoretical Yang-Baxter equation. *Duke Math. J.*, 104(1):1–18, 2000.

[50] H. Meng, A. Ballester-Bolinches, and R. Esteban-Romero. Left braces and the quantum Yang-Baxter equation. *Proc. Edinb. Math. Soc., II. Ser.*, 62(2):595–608, 2019.

[51] K. Nejabati Zenouz. *On Hopf-Galois Structures and Skew Braces of Order p^3*. PhD thesis, The University of Exeter, https://ore.exeter.ac.uk/repository/handle/10871/32248, 2018.

[52] K. Nejabati Zenouz. Skew braces and Hopf-Galois structures of Heisenberg type. *J. Algebra*, 524:187–225, 2019.

[53] D. S. Passman. *The algebraic structure of group rings*. Robert E. Krieger Publishing Co., Inc., Melbourne, FL, 1985. Reprint of the 1977 original.

[54] S. D. Promislow. A simple example of a torsion-free non unique product group. *Bull. Lond. Math. Soc.*, 20(4):302–304, 1988.

[55] W. Rump. Braces, radical rings, and the quatum Yang-Baxter equation. *J. Algebra*, 307(1):153–170, 2007.

[56] W. Rump. Classification of cyclic braces. *J. Pure Appl. Algebra*, 209(3):671–685, 2007.

[57] W. Rump. The brace of a classical group. *Note Mat.*, 34(1):115–145, 2014.

[58] W. Rump. Quasi-linear cycle sets and the retraction problem for set-theoretic solutions of the quantum Yang-Baxter equation. *Algebra Colloq.*, 23(1):149–166, 2016.

[59] W. Rump. Classification of cyclic braces. II. *Trans. Am. Math. Soc.*, 372(1):305–328, 2019.

[60] A. Smoktunowicz. A note on set-theoretic solutions of the Yang-Baxter equation. *J. Algebra*, 500:3–18, 2018.

[61] A. Smoktunowicz. On Engel groups, nilpotent groups, rings, braces and the Yang-Baxter equation. *Trans. Am. Math. Soc.*, 370(9):6535–6564, 2018.

[62] A. Smoktunowicz and A. Smoktunowicz. Set-theoretic solutions of the Yang-Baxter equation and new classes of R-matrices. *Linear Algebra Appl.*, 546:86–114, 2018.

[63] A. Smoktunowicz and L. Vendramin. On skew braces (with an appendix by N. Byott and L. Vendramin). *J. Comb. Algebra*, 2(1):47–86, 2018.

[64] A. Soloviev. Non-unitary set-theoretical solutions to the quantum Yang-Baxter equation. *Math. Res. Lett.*, 7(5-6):577–596, 2000.

[65] A. Szczepański. *Geometry of crystallographic groups*, volume 4 of *Algebra and Discrete Mathematics*. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2012.

[66] M. Tărnauceanu. An arithmetic method of counting the subgroups of a finite Abelian group. *Bull. Math. Soc. Sci. Math. Roum., Nouv. Sér.*, 53(4):373–386, 2010.

[67] L. Vendramin. Extensions of set-theoretic solutions of the Yang-Baxter equation and a conjecture of Gateva-Ivanova. *J. Pure Appl. Algebra*, 220(5):2064–2076, 2016.

[68] L. Vendramin. Problems on skew left braces. *Adv. Group Theory Appl.*, 7:15–37, 2019.

[69] L. Vendramin and A. Konovalov. YangBaxter, combinatorial solutions for the Yang-Baxter equation, version 0.9.0 (2019). Available at https://gap-packages.github.io/YangBaxter.